PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-073414
(43)Date of publication of application : 18.03.1997

(51)Int.Cl. G06F 12/14
G09C 1/00
G11B 20/10
G11B 20/12
G11B 20/18

(21)Application number : 08-098949
(22)Date of filing : 19.04.1996

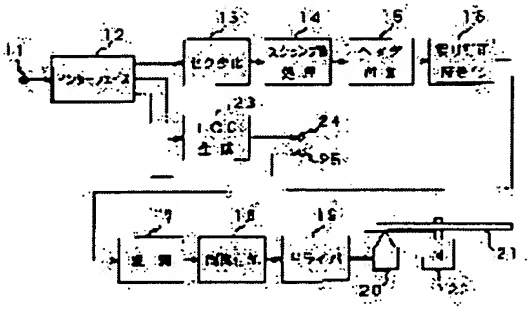
(71)Applicant : SONY CORP
(72)Inventor : SAKO YOICHIRO
KAWASHIMA ISAO
KURIHARA AKIRA
OSAWA YOSHITOMO
OWA HIDEO

(30)Priority

Priority number : 07166698 Priority date : 30.06.1995 Priority country : JP
07187967 30.06.1995 JP

(54) METHOD AND DEVICE FOR DATA RECORDING, DATA RECORDING MEDIUM, AND METHOD AND DEVICE FOR DATA REPRODUCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To cipher data so that it is difficult to decipher the data by using simple constitution.
SOLUTION: An input is ciphered and outputted by at least one circuit among a sectoring circuit 13 which is used to process the input data into a recording signal, a scrambling processing circuit 14, a header adding circuit 15, an error correcting and encoding circuit 16, a modulating circuit 16, a modulating circuit 18, and a synchronism adding circuit 18. In this case, not only the key of the ciphering process itself in the circuit, but also which circuit has performed the ciphering process become a ciphering key.



LEGAL STATUS

[Date of request for examination] 19.07.2001
[Date of sending the examiner's decision of rejection] 13.09.2005
[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-19837

[Date of requesting appeal against examiner's decision of rejection] 13.10.2005

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－73414

(43)公開日　平成９年(1997)３月18日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｇ１１Ｂ	20/10		7736－5Ｄ	Ｇ１１Ｂ	20/10	Ｈ
	20/12	１０２	9295－5Ｄ		20/12	１０２
	20/18	５７０	9558－5Ｄ		20/18	５７０Ｎ

審査請求　未請求　請求項の数33　ＯＬ　（全 28 頁）

(21)出願番号　特願平8－98949

(22)出願日　平成８年(1996)４月19日

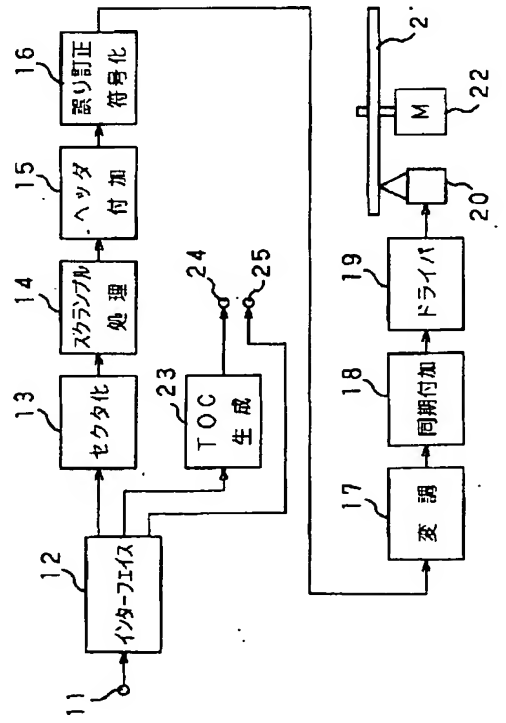
(31)優先権主張番号　特願平7－166698
(32)優先日　平７(1995)６月30日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平7－187967
(32)優先日　平７(1995)６月30日
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　川鳴　功
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　小池　晃　（外２名）

最終頁に続く

(54)【発明の名称】　データ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置

(57)【要約】
【課題】　簡単な構成で、解読が困難な暗号化を施す。
【解決手段】　入力データを処理して記録信号とするために用いられるセクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１８、及び同期付加回路１８の内、いずれか少なくとも１つの回路で、入力に対して暗号化処理を施して出力する。回路内での暗号化処理自体の鍵のみならず、どの回路で暗号化処理を行ったかも暗号化の鍵となる。



【特許請求の範囲】

【請求項１】　入力ディジタルデータを所定データ量単位でセクタ化するセクタ化工程と、
このセクタ化されたディジタルデータにヘッダを付加するヘッダ付加工程と、
このヘッダ付加されたディジタルデータに誤り訂正符号を付加する誤り訂正符号化工程と、
この誤り訂正符号化されたディジタルデータを所定の変調方式で変調する変調工程と、
この変調されたディジタル信号に同期パターンを付加する同期付加工程と、
この同期パターンが付加されたディジタル信号を記録媒体に記録する記録工程とを有し、
上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、及び同期付加工程のいずれか少なくとも１つの工程について、入力に対して暗号化処理を施して出力することを特徴とするデータ記録方法。

【請求項２】　上記セクタ化工程でセクタ化されたディジタルデータ又は上記ヘッダ付加工程でヘッダが付加されたディジタルデータに対して、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を設け、
上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、同期付加工程、及びスクランブル処理工程のいずれか少なくとも１つの工程について、入力に対して暗号化処理を施して出力することを特徴とする請求項１記載のデータ記録方法。

【請求項３】　上記暗号化処理に用いられる鍵情報を複数設定しておき、これらの鍵情報を所定タイミングで切り換えることを特徴とする請求項１記載のデータ記録方法。

【請求項４】　上記セクタ化工程、ヘッダ付加工程、誤り訂正符号化工程、変調工程、及び同期付加工程のいずれの工程で暗号化処理が施されたかを鍵情報とすることを特徴とする請求項１記載のデータ記録方法。

【請求項５】　上記誤り訂正符号化工程の誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴とする請求項１記載のデータ記録方法。

【請求項６】　上記誤り訂正符号は積符号であることを特徴とする請求項１記載のデータ記録方法。

【請求項７】　入力ディジタルデータを所定データ量単位でセクタ化するセクタ化手段と、
このセクタ化手段から出力されたディジタルデータにヘッダを付加するヘッダ付加手段と、
このヘッダ付加手段から出力されたディジタルデータに誤り訂正符号を付加する誤り訂正符号化手段と、
この誤り訂正符号化手段から出力されたディジタルデータを所定の変調方式で変調する変調手段と、
この変調手段から出力されたディジタル信号に同期パターンを付加する同期付加手段と、
この同期付加手段から出力されたディジタル信号を記録媒体に記録する記録手段とを有し、
上記セクタ化手段、ヘッダ付加手段、誤り訂正符号化手段、変調手段、及び同期付加手段のいずれか少なくとも１つの手段は、入力に対して暗号化処理を施して出力することを特徴とするデータ記録装置。

【請求項８】　上記セクタ化手段でセクタ化されたディジタルデータ又は上記ヘッダ付加手段でヘッダが付加されたディジタルデータに対して、同一パターンを除去するためのランダム化処理を施すスクランブル処理手段を設け、
上記セクタ化手段、ヘッダ付加手段、誤り訂正符号化手段、変調手段、同期付加手段、及びスクランブル処理手段のいずれか少なくとも１つの手段は、入力に対して暗号化処理を施して出力することを特徴とする請求項７記載のデータ記録装置。

【請求項９】　上記誤り訂正符号化手段は、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すデータ変換手段を有することを特徴とする請求項７記載のデータ記録装置。

【請求項１０】　入力ディジタルデータが所定データ量単位でセクタ化され、ヘッダが付加され、誤り訂正符号化され、所定の変調方式で変調され、同期パターンが付加されると共に、これらのセクタ化、ヘッダ付加、誤り訂正符号化、変調、及び同期付加のいずれかの際に、入力に対して暗号化処理が施された信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項１１】　データ記録媒体から読み取られたディジタル信号から同期信号を分離する同期分離工程と、
この同期分離されたディジタル信号に対して所定の変調方式に従った復調を施す復調工程と、
この復調されて得られたディジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化工程と、
この誤り訂正復号化処理されたディジタルデータを所定のセクタに分解するセクタ分解工程と、
このセクタ分解されたディジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離工程とを有し、
上記同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、及びヘッダ分離工程の内、いずれか少なくとも１つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施して出力することを特徴とするデータ再生方法。

【請求項１２】　上記セクタ分解工程でセクタに分解されたディジタルデータ又は上記ヘッダ分離工程でヘッダが分離されたディジタルデータに対して、記録時のスクランブルを解くデスクランブル処理工程を設け、

上記同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、ヘッダ分離工程、及びデスクランブル処理工程の内、いずれか少なくとも１つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施して出力することを特徴とする請求項１１記載のデータ再生方法。

【請求項１３】　記録媒体から読み取られたディジタル信号から同期信号を分離する同期分離手段と、
この同期分離手段から出力されたディジタル信号に対して所定の変調方式に従った復調を施す復調手段と、
この復調手段から得られたディジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化手段と、
この誤り訂正復号化手段から出力されたディジタルデータを所定のセクタに分解するセクタ分解手段と、
このセクタ分解手段から出力されたディジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離手段とを有し、
上記同期分離手段、復調手段、誤り訂正復号化手段、セクタ分解手段、及びヘッダ分離手段の内、いずれか少なくとも１つの手段に対応する記録時の工程ついて暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の手段にて、入力に対して暗号の復号化処理を施して出力することを特徴とするデータ再生装置。

【請求項１４】　上記セクタ分解手段から出力されたディジタルデータ又は上記ヘッダ分離手段から出力されたディジタルデータに対して、記録時のスクランブルを解くデスクランブル処理を施すデスクランブル処理手段を設け、
上記同期分離手段、復調手段、誤り訂正復号化手段、セクタ分解手段、ヘッダ分離手段、及びデスクランブル処理手段の内、いずれか少なくとも１つの手段に対応する記録時の手段について暗号化処理が施されており、この記録時に暗号化処理が施された手段に対応する再生時の手段について、入力に対して暗号の復号化処理を施して出力することを特徴とする請求項１３記載のデータ再生装置。

【請求項１５】　入力ディジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録方法において、
上記誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴とするデータ記録方法。

【請求項１６】　上記データ変換は、データと上記鍵情報との論理演算、鍵情報を用いた置換、転置、あるいは関数演算の少なくとも１つにより行われることを特徴とする請求項１５記載のデータ記録方法。

【請求項１７】　上記データ変換を施すデータの個数を暗号化の難易度に応じて変化させることを特徴とする請求項１５記載のデータ記録方法。

【請求項１８】　入力ディジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録装置において、
暗号化の鍵情報の入力手段と、
この入力手段からの鍵情報に応じて、上記誤り訂正符号化処理の際に取り扱われるデータの少なくとも一部に対してデータ変換を施す手段とを有することを特徴とするデータ記録装置。

【請求項１９】　入力ディジタルデータに誤り訂正符号化処理を施す際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換が施されて得られた信号が記録されて成ることを特徴とするデータ記録媒体。

【請求項２０】　誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生方法において、
上記誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換が施されており、
上記誤り訂正符号化処理に対応する誤り訂正復号化処理の際に取り扱われるデータの内の上記暗号化の鍵情報に応じたデータに上記データ変換に対する逆変換を施すことを特徴とするデータ再生方法。

【請求項２１】　誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生装置において、
上記誤り訂正符号化処理の際に取り扱われるデータの内のデータ変換が施されたデータを示す暗号化の鍵情報を入力する鍵情報入力手段と、
上記誤り訂正符号化処理に対応する誤り訂正復号化処理を行うと共に、上記鍵情報入力手段からの暗号化の鍵情報に応じたデータに上記データ変換に対する逆変換を施す誤り訂正復号化手段とを有することを特徴とするデータ再生装置。

【請求項２２】　入力データに対して記録のための信号処理を施して記録媒体の所定のデータ記録領域に記録するデータ記録方法において、
所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として上記記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることを特徴とするデータ記録方法。

【請求項２３】　上記鍵情報として、媒体固有の識別情報、記録装置固有の識別情報、媒体製造装置固有の識別情報、製造者／販売者の識別情報、地域情報、外部から供給される識別情報、の少なくとも１つを用いることを特徴とする請求項１２記載のデータ記録方法。

【請求項２４】　入力データに対して記録のための信号処理を施して記録媒体の所定のデータ記録領域に記録す

るデータ記録装置において、
所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として上記記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることを特徴とするデータ記録装置。
【請求項２５】　データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて暗号化処理が施されたデータが上記データ記録領域に書き込まれて成ることを特徴とするデータ記録媒体。
【請求項２６】　データ記録媒体のデータ記録領域から読み取られ、記録時に暗号化処理の施されたディジタル信号に対して再生のための信号処理を施す際に、
上記データ記録媒体の上記データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことを特徴とするデータ再生方法。
【請求項２７】　上記鍵情報として、媒体固有の識別情報、記録装置固有の識別情報、媒体製造装置固有の識別情報、製造者／販売者の識別情報、再生装置固有の識別情報、地域情報、外部から供給される識別情報、の少なくとも１つを用いることを特徴とする請求項２６記載のデータ再生方法。
【請求項２８】　データ記録媒体のデータ記録領域から読み取られ、記録時に暗号化処理の施されたディジタル信号に対して再生のための信号処理を施すデータ再生装置であって、
上記データ記録媒体の上記データ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことを特徴とするデータ再生装置。
【請求項２９】　入力ディジタルデータを所定データ量単位でセクタ化するセクタ化工程と、
このセクタ化されたディジタルデータに対してスクランブル処理を施すスクランブル処理工程と、
このスクランブル処理されたディジタルデータにヘッダを付加するヘッダ付加工程と、
このヘッダ付加されたディジタルデータに誤り訂正符号を付加する誤り訂正符号化工程と、
この誤り訂正符号化されたディジタルデータを所定の変調方式で変調する変調工程と、
この変調されたディジタル信号に同期パターンを付加する同期付加工程と、
この同期パターンが付加されたディジタル信号を記録媒体に記録する記録工程とを有し、
上記スクランブル処理工程の初期値及び生成多項式の少なくとも一方を暗号化の鍵情報に応じて変化させることを特徴とするデータ記録方法。
【請求項３０】　入力ディジタルデータを所定データ量単位でセクタ化するセクタ化手段と、
このセクタ化手段から出力されたディジタルデータに対して、初期値及び生成多項式の少なくとも一方が暗号化の鍵情報に応じて変化するスクランブル処理を施すスクランブル処理手段と、
このスクランブル処理手段から出力されたディジタルデータにヘッダを付加するヘッダ付加手段と、
このヘッダ付加手段から出力されたディジタルデータに誤り訂正符号を付加する誤り訂正符号化手段と、
この誤り訂正符号化手段から出力されたディジタルデータを所定の変調方式で変調する変調手段と、
この変調手段から出力されたディジタル信号に同期パターンを付加する同期付加手段と、
この同期付加手段から出力されたディジタル信号を記録媒体に記録する記録手段とを有することを特徴とするデータ記録装置。
【請求項３１】　入力ディジタルデータが所定データ量単位でセクタ化され、初期値及び生成多項式の少なくとも一方が暗号化の鍵情報に応じて変化させられたスクランブル処理が施され、ヘッダが付加され、誤り訂正符号化され、所定の変調方式で変調された信号が記録されて成ることを特徴とするデータ記録媒体。
【請求項３２】　データ記録媒体から読み取られたディジタル信号から同期信号を分離する同期分離工程と、
この同期分離されたディジタル信号に対して所定の変調方式に従った復調を施す復調工程と、
この復調されて得られたディジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化工程と、
この誤り訂正復号化処理されたディジタルデータを所定のセクタに分解するセクタ分解工程と、
このセクタ分解されたディジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離工程と、
このヘッダ分離されたディジタルデータに対して記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すデスクランブル処理工程とを有することを特徴とするデータ再生方法。
【請求項３３】　記録媒体から読み取られたディジタル信号から同期信号を分離する同期分離手段と、
この同期分離手段から出力されたディジタル信号に対して所定の変調方式に従った復調を施す復調手段と、
この復調手段から得られたディジタルデータに対して誤り訂正復号化処理を施す誤り訂正復号化手段と、
この誤り訂正復号化手段から出力されたディジタルデータを所定のセクタに分解するセクタ分解手段と、
このセクタ分解手段から出力されたディジタルデータのセクタ構造のヘッダ部分を分離するヘッダ分離手段と、
このヘッダ分離手段から出力されたディジタルデータに対して記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すデスクランブル処理手段とを有することを特徴とするデータ再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コピー防止や不正使用の阻止、あるいは課金システムに適用可能なデータ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置に関する。

【０００２】

【従来の技術】近年において、光ディスク等のディジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる弊害が生じてきているのが実情である。

【０００３】

【発明が解決しようとする課題】ところで、ディジタルオーディオデータやディジタルビデオデータの不法コピー等を回避するためには、いわゆるＳＣＭＳ（シリアルコピー管理システム）やＣＧＭＳ（コピー世代管理システム）の規格が知られているが、これは記録データの特定部分にコピー禁止フラグを立てるようなものであるため、ディジタル２値信号の丸ごとコピーであるいわゆるダンプコピー等の方法によりデータを抜き出される問題がある。

【０００４】また、例えば特開昭６０－１１６０３０号公報に開示されているように、コンピュータデータの場合には、ファイル内容自体を暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。これは、情報流通の形態として、情報が暗号化されて記録されたディジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものであるが、簡単で有用な暗号化の手法の確立が望まれている。

【０００５】本発明は、上述したような実情に鑑みてなされたものであり、簡単な構成で暗号化が行え、データの暗号化によりコピー防止や不正使用の防止が簡単な仕組みで実現でき、暗号の解読が困難であり、また、暗号の難易度あるいは深度の制御も容易に行えるようなデータ記録方法及び装置、データ記録媒体、並びにデータ再生方法及び装置の提供を目的とする。

【０００６】

【課題を解決するための手段】上記の課題を解決するために、本発明に係るデータ記録方法は、入力ディジタルデータを所定データ量単位でセクタ化するセクタ化工程と、ヘッダを付加するヘッダ付加工程と、誤り訂正符号化工程と、所定の変調方式で変調する変調工程と、同期パターンを付加する同期付加工程との、いずれか少なくとも１つの工程について、入力に対して暗号化処理を施して出力することを特徴とすることにより、上述の課題を解決する。これらの暗号化処理が施され得る工程の１つに、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を含めてもよい。

【０００７】このデータ記録方法をデータ記録装置に適用することができる。

【０００８】上記データ記録方法で得られた信号が記録されたデータ記録媒体を提供することができる。

【０００９】本発明に係るデータ再生方法は、上記データ記録方法で記録されたデータ記録媒体を再生する際に、同期分離工程、復調工程、誤り訂正復号化工程、セクタ分解工程、及びヘッダ分離工程の内、いずれか少なくとも１つの工程に対応する記録時の工程について暗号化処理が施されており、この記録時に暗号化処理が施された工程に対応する再生時の工程について、入力に対して暗号の復号化処理を施すことにより、上述の課題を解決する。これらの暗号復号化処理が施され得る工程の１つに、記録時のスクランブルを解くデスクランブル処理を施すスクランブル処理工程を含めてもよい。

【００１０】このデータ再生方法をデータ再生装置に適用することができる。

【００１１】また、本発明に係るデータ記録方法は、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施すことを特徴としている。このデータ変換としては、データと上記鍵情報との論理演算や、転置、置換等を挙げることができる。

【００１２】また、本発明に係るデータ記録方法は、所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部として記録媒体のデータ記録領域とは別の領域に書き込まれた情報を用いることにより、上述の課題を解決する。これをデータ記録装置、データ記録媒体に適用することができる。

【００１３】また、本発明に係るデータ再生方法は、記録時に暗号化処理の施されたディジタル信号に対して再生のための信号処理を施す際に、データ記録媒体のデータ記録領域とは別の領域に書き込まれた情報が少なくとも一部とされた鍵情報を用いて、暗号復号化処理を施すことにより、上述の課題を解決する。これをデータ再生装置に適用することができる。

【００１４】さらに、本発明に係るデータ記録方法は、スクランブル処理工程の初期値及び生成多項式の少なくとも一方を暗号化の鍵情報に応じて変化させることにより、上述の課題を解決する。

【００１５】また、本発明に係るデータ再生方法は、記録時の暗号化の鍵情報により初期値及び生成多項式の少なくとも一方を変化させてスクランブルを解くデスクランブル処理を施すことにより、上述の課題を解決する。

【００１６】入力ディジタルデータを所定データ量単位でセクタ化し、ヘッダを付加し、誤り訂正符号化処理を施し、所定の変調方式で変調し、同期パターンを付加して、記録媒体に記録する。これらの工程のいずれか少なくとも１つの工程について、入力に対して暗号化処理を施して出力することにより、どの工程で暗号化処理が施されたかも暗号の鍵となり、暗号の難易度が高くなる。

【００１７】暗号化の鍵情報の少なくとも一部を、記録媒体のデータ記録領域とは別の領域に書き込んでおき、再生時にこの鍵情報の少なくとも一部の情報を読み取って、暗号復号化に用いる。暗号復号化の鍵情報が、記録媒体のデータ記録領域内の情報のみで完結しないため、暗号化の難易度が高まる。

【００１８】データ列の同一パターンを除去するためのランダム化を主目的とするスクランブル処理の際に、生成多項式及び初期値の少なくとも一方を、暗号化の鍵に応じて変化させる。既存のスクランブル処理を暗号化に流用できる。

【００１９】

【発明の実施の形態】以下、本発明に係るいくつかの好ましい実施の形態について、図面を参照しながら説明する。

【００２０】図１は、本発明の第１の実施の形態を概略的に示すブロック図である。この図１において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、インターフェース回路１２を介して、セクタ化回路１３に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。セクタ化されたデータは、スクランブル処理回路１４に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路１５に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路１６に送られる。誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ１９を介して記録ヘッド２０に送っている。記録ヘッド２０は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体２１に上記変調された記録信号の記録を行う。このディスク状記録媒体２１は、スピンドルモータ２２により回転駆動される。

【００２１】なお、上記スクランブル処理回路１４は、必須ではなく、また、ヘッダ付加回路１５の後段に挿入して、ヘッダ付加されたディジタルデータに対してスクランブル処理を施して誤り訂正符号化回路１６に送るようにしてもよい。

【００２２】ここで、セクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路は、入力に対して暗号化処理を施して出力するような構成を有している。好ましくは、２つ以上の回路で暗号化処理を施すことが挙げられる。この暗号化処理の鍵情報は、記録媒体２１のデータ記録領域とは別の領域に書き込まれた識別情報、例えば媒体固有の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、国別コード等の地域情報、外部から供給される識別情報等を少なくとも一部に用いている。このように、媒体のデータ記録領域以外に書き込まれる識別情報は、例えば上記インターフェース回路１２からＴＯＣ（Table of contents ）生成回路２３を介して端子２４に送られる情報であり、また、インターフェース回路１２から直接的に端子２５に送られる情報である。これらの端子２４、２５からの識別情報が、暗号化の際の鍵情報の一部として用いられ、回路１３～１８の少なくとも１つ、好ましくは２以上で、この鍵情報を用いた入力データに対する暗号化処理が施される。

【００２３】この場合、回路１３～１８のどの回路において暗号化処理が施されたかも選択肢の１つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、１つの回路で暗号化処理が施されていれば、６つの選択肢の１つを選ぶことが必要となり、２つの回路で暗号化処理が施されていれば、２つの回路の組み合わせの数に相当する１５個の選択肢の内から１つを選ぶことが必要となる。６つの回路１３～１８の内の１～６つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。

【００２４】また、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることが挙げられる。この所定タイミングで鍵情報の切り換える場合に、切り換えを行うか否かや、切換周期、複数の鍵情報の切換順序等の情報も鍵として用いることができ、暗号化のレベルあるいは暗号の難易度、解き難さ、解読の困難さをさらに高めることができる。

【００２５】次に、各回路１３～１８の構成及び暗号化処理の具体例について説明する。

【００２６】先ず、セクタ化回路１３においては、例えば図２に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図２において、上記図１のインターフェース回路１２からの出力を、２出力の切換スイッチ３１に送り、この切換スイッチ３１の一方の出力を偶奇インターリーバ３３を介してセクタ化器３４に送り、切換スイッチ３１の他方の出力をそのままセクタ化器３４に送っている。セクタ化器３４では、例えば入力データの２０４８バイト単位でまとめて１セクタとしている。このセクタ化回路１３の切換スイッチ３２の切換動作を、鍵となる１ビットの制御信号で制御するわけである。偶奇インターリーバ３３は、図３のＡに示すような偶数バイト３６ａと奇数バイト３６ｂとが交互に配置された入力データの１セクタ分を、図３のＢに示すように、偶数データ部３７ａと奇数データ部３７ｂとに分配して出力する。さらに、図３のＣに示すように、１セクタ内の所定の領域３９を鍵情報により特定し、この領域３９内のデータについてのみ偶数データ部３９ａと奇数データ部３９ｂとに分配するようにしてもよい。この場合には、領域３９の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。

【００２７】次に、スクランブル処理回路１４には、例えば図４に示すように、１５ビットのシフトレジスタを用いたいわゆるパラレルブロック同期タイプのスクランブラを用いることができる。このスクランブラのデータ入力用の端子３５には、ＬＳＢ（最下位ビット）が時間的に先となる順序、いわゆるＬＳＢファーストで、上記セクタ化回路１３からのデータが入力される。スクランブル用の１５ビットのシフトレジスタ１４ａは、排他的論理和（ExOR）回路１４ｂを用いて生成多項式$x^{15}+x+1$に従ったフィードバックがかけられ、１５ビットのシフトレジスタ１４ａには、図５に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図５のプリセット値の選択番号は、例えばセクタアドレスの下位側４ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ１４ａからの出力データと端子３５からの入力データとは、ExOR回路１４ｃにより排他的論理和がとられて、端子１４ｄより取り出され、図１のヘッダ付加回路１５に送られる。

【００２８】ここで、上記生成多項式及びプリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記生成多項式を変化させるには、例えば図６に示すような構成を用いればよい。この図６において、１５ビットのシフトレジスタ１４ａの各ビットからの出力が切換スイッチ１４ｆの各被選択端子に送られ、この切換スイッチ１４ｆは制御端子１４ｇからの例えば４ビットの制御データによって切換制御され、切換スイッチ１４ｆからの出力はExOR回路１４ｂに送られている。このような構成の制御端子１４ｇの制御データを変化させることにより、生成多項式$x^{15}+x^{n}+1$のｎを変化させることができる。また、上記プリセット値を変化させるには、上記図５のプリセット値テーブルの各プリセット値を、例えば１６バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND ）、論理和（OR）、シフト演算等を使用できる。なお、生成多項式を変化させるための構成は図６の構造に限定されず、シフトレジスタの段数や取り出すタップ数を任意に変更してもよい。

【００２９】次に、ヘッダ付加回路１５について説明する。先ず、図７はセクタフォーマットの具体例を示しており、１セクタは、２０４８バイトのユーザデータ領域４１に対して、４バイトの同期領域４２と、１６バイトのヘッダ領域４３と、４バイトの誤り検出符号（ＥＤＣ）領域４４とが付加されて構成されている。誤り検出符号領域４４の誤り検出符号は、ユーザデータ領域４１及びヘッダ領域４３に対して生成される３２ビットのＣＲＣ符号から成っている。ヘッダ付加回路１５での暗号化処理としては、同期いわゆるデータシンクに対して、ヘッダのアドレス及びＣＲＣに対して施すことが挙げられる。

【００３０】セクタの同期すなわちデータシンクに対して暗号化処理を施す一例としては、４バイトの同期領域４２の各バイトに割り当てられたバイトパターンを、図８の「Ａ」、「Ｂ」、「Ｃ」、「Ｄ」にてそれぞれ表すとき、２ビットの鍵情報を用いて、この４バイトの内容をバイト単位でシフトあるいはローテートすることが挙げられる。すなわち、２ビットの鍵が「０」のとき「ＡＢＣＤ」、「１」のとき「ＢＣＤＡ」、「２」のとき「ＣＤＡＢ」、「３」のとき「ＤＡＢＣ」のように切り換えることにより、この鍵が合致しないとセクタの同期がとれなくなり、正常な再生が行えない。なお、上記バイトパターン「Ａ」～「Ｄ」としては、例えばＩＳＯ６４６のキャラクタコード等を使用できる。

【００３１】ヘッダ領域４３内には、図９に示すように、いわゆる巡回符号であるＣＲＣ４５、コピーの許可／不許可やコピー世代管理等のためのコピー情報４６、多層ディスクのどの層かを示す層４７、アドレス４８、予備４９の各領域が設けられている。この内で、アドレス４８の３２ビットにビットスクランブル、この場合には、ビット単位での転置処理を施すことにより、暗号化

が行える。また、ＣＲＣ４５の生成多項式として、$x^{16}+x^{15}+x^2+1$ が用いられている場合、第２、第３項のx^{15}、x^2 の代わりに、x^{15}～xに対応する１５ビットを鍵に応じて変化させることが挙げられる。また、ＣＲＣ４５の１６ビットと鍵情報とを論理演算することも挙げられる。

【００３２】なお、上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダ、あるいは媒体製造装置の固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【００３３】次に、誤り訂正符号化回路１６の具体例を図１０、図１１に示す。これらの図１０、図１１において、入力端子５１には、上記図１のヘッダ付加回路１５からのデータが第１の符号化器であるＣ１エンコーダ５２に供給されている。この具体例においては、誤り訂正符号化の１フレームは１４８バイトあるいは１４８シンボルのデータから成るものとしており、入力端子５１からのディジタルデータが１４８バイト毎にまとめられて、第１の符号化器であるＣ１エンコーダ５２に供給される。Ｃ１エンコーダ５２では８バイトのＰパリティが付加され、インターリーブのための遅延回路５３を介して第２の符号化器であるＣ２エンコーダ５４に送られる。Ｃ２エンコーダ５４では１４バイトのＱパリティが付加され、このＱパリティは遅延回路５５を介してＣ１エンコーダ５２に帰還されている。このＣ１エンコーダ５２からのＰ、Ｑパリティを含む１７０バイトが取り出されて、遅延回路５６を介し、インバータ部５７ａを有する再配列回路５７を介して出力端子５８より取り出され、図１の変調回路１７に送られる。

【００３４】このような誤り訂正符号化回路において暗号化処理を施す場合には、例えば再配列回路５７内のインバータ部５７ａの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、２２バイトのＰ、Ｑパリティに対して再配列回路５７のインバータ部５７ａのインバータによる反転が行われて出力されるが、これらのインバータのいくつかを無くしたり、Ｃ１データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。

【００３５】このようなデータ変換を施す場合、基準構成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばＣ１エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが９であるため、最大４バイトまでのエラー検出訂正が行え、消失（イレージャ）ポインタがあれば最大８バイトまでの訂正が可能であることから、違いが５箇所以上あると、Ｃ１符号では常に訂正不可又は誤訂正となる。違いが４箇所の場合は、他に１バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが３、２、１箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【００３６】この場合、予めインバータの変更を行う場所を例えば２箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を２箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【００３７】さらに、インバータの挿入あるいは変更位置としては、図１０、図１１の再配列回路５７内の位置に限定されず、例えばＣ１エンコーダ５２の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、上記データ変換としては、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしたり、データを暗号化の鍵情報に応じて転置するようにしたり、データを暗号化の鍵情報に応じて置換するようにしてもよい。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【００３８】ここで、図１２は、上記誤り訂正符号化回路１６の他の具体例として、再配列回路５７内のインバータ部５７ａの後段の位置に排他的論理和（ExOR）回路群６１を挿入し、Ｃ１エンコーダ５２の前段すなわち入力側の位置にもExOR回路群６６を挿入した例を示している。

【００３９】具体的に、ExOR回路群６１は、Ｃ１エンコーダ５２から遅延回路５６、及び上記再配列回路５７のインバータ部５７ａを介して取り出される１７０バイトのデータ、すなわち情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$のデータに対して排他的論理和（ExOR）回路を用いたデータ変換を行い、ExOR回路群６６は、１４８バイトの入力データB_{148n}～$B_{148n+147}$に対して排他的論理和（ExOR）回路を用いたデータ変換を行う。これらのExOR回路群６１、６６に用いられるExOR回路は、１バイトすなわち８ビットの入力データと１ビットの制御データで指示される所定の８ビットデータとの排他的論理和（ExOR）をそれぞれとるような８ビットExOR回路であり、このような８ビットExOR回路（所定の８ビットデータがオール１の場合はインバー

タ回路に相当する）が、ExOR回路群６１では１７０個、ExOR回路群６６では１４８個用いられている。

【００４０】この図１２においては、１７０ビットの鍵情報が端子６２に供給され、いわゆるＤラッチ回路６３を介してExOR回路群６１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路６３は、イネーブル端子６４に供給された１ビットの暗号化制御信号に応じて、端子６２からの１７０ビットの鍵情報をそのままExOR回路群６１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。ExOR回路群６１の１７０個の各ExOR回路の内、Ｄラッチ回路６３から“０”が送られたExOR回路は、再配列回路５７内のインバータ部５７ａからのデータをそのまま出力し、Ｄラッチ回路６３から“１”が送られたExOR回路は、再配列回路５７内のインバータ部５７ａからのデータを反転して出力する。オールゼロのときには、再配列回路５７内のインバータ部５７ａからのデータをそのまま出力することになる。また、ExOR回路群６６については、１４８個のExOR回路を有し、鍵情報が１４８ビットであること以外は、上記ExOR回路群６１の場合と同様であり、端子６７に供給された１４８ビットの鍵情報がＤラッチ回路６８を介してExOR回路群６６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路６８はイネーブル端子６９の暗号化制御信号により１４８ビットの鍵情報かオールゼロかが切換制御される。

【００４１】この図１２の例において、ExOR回路群６１は、Ｃ１エンコーダ５２から遅延回路５６、インバータ部５７ａを介して取り出される１７０バイトのデータとしての情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$のデータに対して排他的論理和（ExOR）回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り１４８バイトの情報データ$C1_{170n+169}$～$C1_{170n+22}$に対して、１４８ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【００４２】この図１２の回路においても、上記図１０、図１１の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群６１、６６のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【００４３】上記鍵情報は、上述したように、媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダあるいは媒体製造装置の固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができる。

【００４４】なお、上記データ変換手段としてのExOR回路群６１、６６の代わりに、ＡＮＤ、ＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路群等を使用してもよい。また、８ビット単位で１ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、８ビットの情報データに対して８ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの１ワードに相当する８ビットの内の各ビットに対してそれぞれＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用してもよい。この場合には、例えば１４８バイトすなわち１４８×８ビットのデータに対して、１４８×８ビットの鍵データが用いられることになり、さらにＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【００４５】さらに、この第１の実施の形態においては、クロスインターリーブ型の誤り訂正符号の例について説明したが、積符号の場合にも同様に適用可能であり、これについては本発明の第２の実施の形態として後述する。

【００４６】次に、図１の変調回路１７での暗号化処理について、図１３を参照しながら説明する。この図１３において、入力端子７１には、上記誤り訂正符号化回路１６からのデータが８ビット（１バイト）毎に供給され、入力端子７２には８ビットの鍵情報が供給されており、これらの８ビットデータは、論理演算回路の一例としてのExOR回路７３に送られて排他的論理和がとられる。このExOR回路７３からの８ビット出力が、所定の変調方式の変調器、例えば８－１６変換回路７４に送られて、１６チャンネルビットに変換される。この８－１６変換回路７４での８－１６変調方式の一例としてはいわゆるＥＦＭプラス変調方式が挙げられる。

【００４７】この図１３の例では、データ変調の前に８ビットの鍵情報を用いた暗号化処理を施しているが、鍵情報のビット数は８ビットに限定されず、また、８－１６変調の際の変換テーブルの入出力の対応関係を鍵情報に応じて変化させるようにしてもよい。鍵情報には、上述した媒体固有の識別情報等を使用できることは勿論である。

【００４８】次に、同期付加回路１８について説明する。同期付加回路１８では、例えば図１４に示すような４種類の同期ワードＳ０～Ｓ３を用いて、上記８－１６変調のフレーム単位で同期をとっている。この８－１６変調フレーム（例えばＥＦＭプラスフレーム）は、例えば８５データシンボルである１３６０チャンネルビットから成り、この１フレーム１３６０チャンネルビット毎

に３２チャンネルビットの同期ワードが付加されると共に、このフレームを上記Ｃ１符号やＣ２符号に対応させて構造化し、Ｃ１符号系列の先頭フレームの同期ワードと他のフレームの同期ワードを異ならせる等して、上記４種類の同期ワードＳ０～Ｓ３を使い分けている。これらの同期ワードＳ０～Ｓ３は、直前のワードの“１”、“０”の状態やいわゆるデジタルサムあるいは直流値等に応じてそれぞれ２つの同期パターンａ、ｂを有している。

【００４９】このような４種類の同期ワードＳ０～Ｓ３の選択を、例えば図１５に示すような回路を用いて、２ビットの鍵情報７５に応じて変更することにより、暗号化が行える。すなわち、上記４種類の同期ワードＳ０～Ｓ３を指定する２ビットデータ７６の各ビットと、上記２ビットの鍵情報７５の各ビットとが、２つのExOR回路７７、７８によりそれぞれ排他的論理和され、新たな同期ワード指定データ７９となる。これにより、上記フレーム構造における同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が変更され、暗号化がなされることになる。

【００５０】なお、同期ワードの種類数をさらに増やしてそれらの内から４種類の同期ワードを取り出す取り出し方を暗号化の鍵により決定するようにしてもよい。この鍵情報としては、上述した媒体固有の識別情報等が使用できる。

【００５１】次に図１６は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents ）領域となるリードイン（leadin ）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００５２】上記鍵情報の一部として、データ記録領域であるプログラム領域１０４以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、ＴＯＣ領域であるリードイン領域１０３や、リードアウト領域１０５に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにすると共に、これを鍵情報として、上述した６つの回路１３～１８の少なくとも１つ、好ましくは２つ以上で暗号化処理を施して得られた信号をデータ記録領域であるプログラム領域１０４に記録するようにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域１０３よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【００５３】次に、本発明のデータ再生方法、データ再生装置の実施の形態について、図１７を参照しながら説明する。

【００５４】図１７において、記録媒体の一例としてのディスク状記録媒体１０１は、スピンドルモータ１０８により回転駆動され、光学ピックアップ装置等の再生ヘッド装置１０９により媒体記録内容が読み取られる。

【００５５】再生ヘッド装置１０９により読み取られたディジタル信号は、ＴＯＣデコーダ１１１及びアンプ１１２に送られる。ＴＯＣデコーダ１１１からは、ディスク状記録媒体１０１の上記リードイン領域１０３にＴＯＣ情報の一部として記録された上記識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報が読み取られ、この識別情報が暗号を復号化するための鍵情報の少なくとも一部として用いられる。この他、再生装置内部のＣＰＵ１２２から、再生装置固有の識別情報や、外部からの識別情報を出力するようにし、この識別情報を鍵情報の少なくとも一部として用いるようにしてもよい。なお、外部からの識別情報としては、通信回線や伝送路等を介して受信された識別情報や、いわゆるＩＣカード、ＲＯＭカード、磁気カード、光カード等を読み取って得られた識別情報等が挙げられる。

【００５６】再生ヘッド装置１０９からアンプ１１２を介し、ＰＬＬ（位相ロックループ）回路１１３を介して取り出されたディジタル信号は、同期分離回路１１４に送られて、上記図１の同期付加回路１８で付加された同期信号の分離が行われる。同期分離回路１１４からのディジタル信号は、復調回路１１５に送られて、上記図１の変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路１１５からのディジタルデータは、誤り訂正復号化回路１１６に送られて、図１の誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路１１７によりセクタに分解され、ヘッダ分離回路１１８により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路１１７及びヘッダ分離回路１１８は、上記図１のセクタ化回路１３及びヘッダ付加回路１５に対応するものである。次に、デスクランブル処理回路１１９により、上記図１のスクランブル処理回路１４におけるスクランブル処理の逆処理としてのデスクランブル処

理が施され、インターフェース回路１２０を介して出力端子１２１より再生データが取り出される。

【００５７】ここで、上述したように、記録時には、上記図１のセクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路において暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路１１４～１１９にて、暗号を復号化する処理が必要とされる。すなわち、上記図１のセクタ化回路１３にて暗号化処理が施されている場合には、セクタ分解回路１１７にて暗号化の際の鍵情報を用いた暗号の復号化処理が必要とされる。以下同様に、図１のスクランブル処理回路１４での暗号化処理に対応してデスクランブル処理回路１１９での暗号復号化処理が、図１のヘッダ付加回路１５での暗号化処理に対応してヘッダ分離回路１１８での暗号復号化処理が、図１の誤り訂正符号化回路１６での暗号化処理に対応して誤り訂正復号化回路１１６での暗号復号化処理が、図１の変調回路１７での暗号化処理に対応して復調回路１１５での暗号復号化処理が、さらに図１の同期付加回路１８での暗号化処理に対応して同期分離回路１１４での暗号復号化処理が、それぞれ必要とされる。

【００５８】同期分離回路１１４での暗号復号化処理は、上記図１４や図１５と共に説明したように、複数種類、例えば４種類の同期ワードの使い方あるいはフレーム構造内での各種同期ワードの使用位置が鍵情報に応じて変更され、暗号化がなされたものを、鍵情報に応じて検出することで行われる。

【００５９】次に、復調回路１１５での暗号復号化処理は、図１８に示すように、同期分離回路１１４から１６－８変換回路１３１に送られて１６チャンネルビットが８ビットデータに変換されたものを、上記図１３のExOR回路７３に対応するExOR回路１３２に送り、端子１３３からの８ビットの鍵情報との排他的論理和をとることで、図１３の入力端子７１に供給された８ビットデータに相当するデータが復元され、これが誤り訂正復号化回路１１６に送られる。

【００６０】次に、誤り訂正復号化回路１１６では、例えば上記図１０、図１１の誤り訂正符号化処理の逆処理が、図１９、図２０の構成により行われる。

【００６１】これらの図１９、図２０において、上記復調回路１１５にて復調されたデータの１７０バイトあるいは１７０シンボルを１まとまりとして、インバータ部１４２ａを有する再配列回路１４２を介し、遅延回路１４３を介して第１の復号器であるＣ１デコーダ１４４に送られている。このＣ１デコーダ１４４に供給される１７０バイトのデータの内２２バイトがＰ，Ｑパリティであり、Ｃ１デコーダ１４４では、これらのパリティデータを用いた誤り訂正復号化が施される。Ｃ１デコーダ１４４からは、１７０バイトのデータが出力されて、遅延回路１４５を介して第２の復号器であるＣ２デコーダ１４６に送られ、パリティデータを用いた誤り訂正復号化が施される。Ｃ２デコーダ１４６からの出力データは、図１９の遅延・Ｃ１デコード回路１４０に送られる。これは、上記遅延回路１４３及びＣ１デコーダ１４４と同様のものであり、これらの遅延回路１４３及びＣ１デコーダ１４４と同様の処理を繰り返し行うことにより誤り訂正復号化を行うものである。図８の例では、遅延回路１４７及び第３の復号器であるＣ３デコーダ１４８で表している。この遅延回路１４７及びＣ３デコーダ１４８、あるいは遅延・Ｃ１デコード回路１４０で最終的な誤り訂正復号化が施され、パリティ無しの１４８バイトのデータが出力端子１４９を介して取り出される。この１４８バイトのデータは、上記図１０、図１１のＣ１エンコーダ５２に入力される１４８バイトのデータに相当するものである。

【００６２】そして、図１０、図１１の誤り訂正符号化回路の再配列回路５７内のインバータ部５７ａで、インバータの有無による暗号化が施されている場合には、図１９、図２０の誤り訂正復号化回路の再配列回路１４２内のインバータ部１４２ａにて、対応する暗号復号化を行うことが必要とされる。この他、図１０、図１１と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【００６３】ここで、図２１は、上記図１２の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【００６４】この図２１において、上記図１２の再配列回路５７内のインバータ部５７ａの出力側に挿入されたExOR回路群６１に対応して、再配列回路１４２のインバータ部１４２ａの入力側及び遅延回路１４３の入力側の位置に、ExOR回路群１５１が挿入され、図１２のＣ１エンコーダ５２の入力側に挿入されたExOR回路群６６に対応して、Ｃ３デコーダ１４８の出力側にExOR回路群１５６が挿入されている。

【００６５】これらのExOR回路群１５１、１５６は、上述したように、図１２のExOR回路群６１、６６によるデータ変換をそれぞれ復号化するためのデータ変換を施すものであり、ExOR回路群１５１は、例えば１７０個の８ビットExOR回路により、またExOR回路群１５６は、１４８個の８ビットExOR回路によりそれぞれ構成されている。なお、記録側の図１２の誤り訂正符号化回路のExOR回路群６１で、パリティデータを除く１４８バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR回路群１５１は１４８個の８ビットExOR回路により構成されることは勿論である。

【００６６】この図２１の端子１５２には、図１２の端子６２に供給される鍵情報に相当する１７０ビットの鍵

情報が供給され、いわゆるＤラッチ回路１５３を介してExOR回路群１５１内の１７０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路１５３は、イネーブル端子１５４に供給された１ビットの暗号化制御信号に応じて、端子１５２からの１７０ビットの鍵情報をそのままExOR回路群１５１に送るか、オールゼロ、すなわち１７０ビットの全てを“０”とするかが切換制御される。また、ExOR回路群１５６については、１４８個のExOR回路を有し、鍵情報が図１２の端子６７に供給される鍵情報と同様の１４８ビットであること以外は、上記ExOR回路群１５１の場合と同様であり、端子１５７に供給された１４８ビットの鍵情報がＤラッチ回路１５８を介してExOR回路群１５６内の１４８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路１５８はイネーブル端子１５９の暗号化制御信号により１４８ビットの鍵情報かオールゼロとするかが切換制御される。

【００６７】このように、誤り訂正回路のインバータやExOR回路等を暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータ等の数を制御することにより、通常でも再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータやExOR回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように１箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆるＬＳＩやＩＣチップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【００６８】次に、セクタ分解回路１１７においては、上記図２、図３と共に説明したように、記録時に上記セクタ化回路１３で偶数・奇数バイトのインターリーブによる暗号化が施されている場合に、この偶奇インターリーブを解くような逆の処理、いわゆるデインターリーブ処理を施すものである。

【００６９】また、ヘッダ分離回路１１８においては、記録時に、上記ヘッダ付加回路１５において、上記図７～図９と共に説明したような暗号化処理、すなわちセクタ同期となるデータシンクのバイトパターンの転置や、アドレス、ＣＲＣの変更がなされている場合に、これを復元するような暗号復号化処理を施すものである。

【００７０】次に、図２２は、デスクランブル処理回路１１９の具体例を示しており、端子１６１には、図１７のヘッダ分離回路１１８からのディジタルデータが供給されている。この端子１６１からのディジタルデータは、例えば上記図４に示すような構成を有するスクランブラ１６３でデスクランブル処理され、出力端子１６４より取り出される。このスクランブラ１６３についての、上記図４と共に説明したような生成多項式１６５及びプリセット値（あるいは初期値）１６６を、認証機構１７１からの暗号の鍵情報に応じて変化させることにより、暗号復号化を行うことができる。この認証機構１７１では、上記ヘッダ情報１６７のコピー情報４６の内容や、媒体固有のあるいは再生装置固有の固有識別情報１７２や、製造者、販売者等の共通識別情報１７３や、外部から与えられる外部識別情報１７４等により、暗号の鍵情報を生成し、この鍵情報に応じて生成多項式１６５やプリセット値１６６を制御する。

【００７１】これらの各回路１１４～１１９のいずれで暗号復号化処理が必要とされるかの情報も、暗号の鍵情報となることは前述した通りである。また、暗号の鍵情報を所定周期、例えばセクタ周期で切り換えることができ、この切換を行うか否かや、切換周期等も鍵とすることにより、暗号化の難易度が高められる。

【００７２】以上説明したように、製造者識別情報、販売者識別情報、装置識別情報等と、別途設定されるコピープロテクト情報、課金情報を組み合わせて、データを暗号化して記録しておくことにより、コピー防止、海賊盤防止、不正使用の防止等を物理フォーマットレベルで実現し得るようにしている。また、データセキュリティ機能の情報、例えばコピーの許可／不許可情報、有償／無償情報を、記録媒体及び記録／再生システムの物理フォーマットにインプリメントしている。

【００７３】すなわち、セキュリティ／課金情報を予め媒体に記録しておき、媒体に記録又は未記録の識別情報を用いて、それをデータの暗号化と組み合わせることにより、簡単な仕組みでコピー防止、不正使用防止が実現できるようになる。また、物理フォーマットにそれを内在させることにより、解読が困難になる。また、ダンプコピーされても暗号化されたままであるので安全である。さらに、セクタ単位やファイル単位、ゾーン単位、レイヤ単位等で可変にできる。またさらに、通信やＩＣカードやリモコン等で鍵がコントロールできる。さらに、海賊盤に対して履歴が残せる。

【００７４】次に、本発明の第２の実施の形態について説明する。この第２の実施の形態は、上述した第１の実施の形態の構成を部分的に変更したものであり、全体の基本構成は、前述した図１に示す通りである。この図１の構成の各回路１３～１８の内の変更部分について以下説明する。

【００７５】図１のセクタ化回路１３は前述した第１の実施の形態と同様に構成すればよいが、スクランブル処理回路１４については、図２３に示す構成を用いている。

【００７６】この図２３に示すスクランブル処理回路１４において、データ入力用の端子３５には、ＬＳＢ（最下位ビット）が時間的に先となる順序、いわゆるＬＳＢファーストで、図１のセクタ化回路１３からのデータが入力される。スクランブル用の１５ビットのシフトレジスタ１４ａは、排他的論理和（ExOR）回路１４ｂを用いて生成多項式 $x^{15}+x^{4}+1$ に従ったフィードバックがかけられ、１５ビットのシフトレジスタ１４ａには、図２４に示すようなプリセット値（あるいは初期値）が設定されるようになっており、図２４のプリセット値の選択番号は、例えばセクタアドレスの下位側４ビットの値に対応させて、セクタ単位でプリセット値が切り換えられるようになっている。シフトレジスタ１４ａからの出力データと端子３５からの入力データとは、ExOR回路１４ｃにより排他的論理和がとられて、端子１４ｄより取り出され、図１のヘッダ付加回路１５に送られる。

【００７７】ここで、上記プリセット値（初期値）を、所定の識別番号等の鍵情報に応じて変化させるようにすることができる。すなわち、上記図２４のプリセット値テーブルの各プリセット値を、例えば１６バイトの識別情報の各バイト値と論理演算することが挙げられる。この場合の識別情報としては、上述したような媒体固有の識別情報、製造元識別情報、販売者識別情報や、記録装置やエンコーダの固有の識別情報、媒体製造装置固有の識別情報、地域情報、外部から供給される識別情報等、あるいはこれらの組み合わせや他の情報との組み合わせ等を用いることができ、また上記論理演算としては、排他的論理和（ExOR）や、論理積（AND）、論理和（OR）、シフト演算等を使用できる。

【００７８】次に、この第２の実施の形態のセクタフォーマットとしては、例えば、図２５に示すようなものを用いている。

【００７９】この図２５に示すように、１セクタは、１行１７２バイトの１２行、すなわち２０６４バイトから成り、この中にメインデータ２０４８バイトを含んでいる。１２行の最初の行の先頭位置には、４バイトのＩＤ（識別データ）と、２バイトのＩＥＤ（ＩＤエラー検出符号）と、６バイトのＲＳＶ（予備）とがこの順に配置されており、最後の行の終端位置には、４バイトのＥＤＣ（エラー検出符号）が配置されている。

【００８０】上記ＩＤ（識別データ）の４バイトは、図２６に示すように、ＭＳＢ側の最初のバイト（ビットｂ３１～ｂ２４）はセクタ情報から成り、残りの３バイト（ビットｂ２３～ｂ０）はセクタ番号から成っている。セクタ情報は、ＭＳＢ側から順に、１ビットのセクタフォーマットタイプ、１ビットのトラッキング方法、１ビットの反射率、１ビットの予備、２ビットのエリアタイプ、２ビットの層番号の各情報から成っている。

【００８１】図１のヘッダ付加回路１５では、このようなセクタフォーマットにおいて、例えば上記ＩＤ（識別データ）の内のセクタ番号の２４ビットに対して、上記鍵情報に応じて例えばビット単位でのスクランブル処理である転置処理を施すことにより、暗号化を施すことができる。また、上記２バイトのＩＥＤ（ＩＤエラー検出符号）の生成多項式や、４バイトのＥＤＣ（エラー検出符号）の生成多項式等を上記鍵情報に応じて変更することによっても、あるいはこれらの情報と鍵情報とを論理演算することによっても、暗号化を施すことができる。

【００８２】次に、図１の誤り訂正符号化回路１６としては、図２７に示すような構成の回路が用いられる。この符号化は、図２８に示すような積符号あるいはブロック符号が用いられる。図２７において、入力端子２１０には、前記図１のヘッダ付加回路１５からのデータが供給され、この入力データは、第１の符号化器であるＰＯエンコーダ２１１に送られる。このＰＯエンコーダ２１１への入力データは、図２８に示すように、$B_{0,0}$～$B_{191,171}$の１７２バイト×１９２行のデータであり、ＰＯエンコーダ２１１では、１７２列の各列１９２バイトのデータに対して、それぞれ１６バイトずつのリード・ソロモン（ＲＳ）符号としてのＲＳ（208,192,17）の外符号（ＰＯ）を付加している。ＰＯエンコーダ２１１からの出力データは、前述したような暗号化のためのデータ変換回路２１２を介して、インターリーブ回路２１３に送られてインターリーブ処理され、ＰＩエンコーダ２１４に送られる。このＰＩエンコーダ２１４では、図２８に示すように、上記ＰＯパリティが付加された１７２バイト×２０８行のデータの各行の１７２バイトのデータに対して、それぞれ１０バイトずつのＲＳ（182,172,11）の内符号（ＰＩ）を付加している。従って、このＰＩエンコーダ２１４からは、１８２バイト×２０８行のデータが出力されることになる。この出力データは、前述したような暗号化のためのデータ変換回路２１５を介して、出力端子２１６より取り出される。

【００８３】ここで、データ変換回路２１２については、ＰＯエンコーダ２１１が各列毎の１９２バイトの入力データに対して１６バイトのＰＯパリティを付加して２０８バイトのデータを出力することから、この１６バイトのパリティに対して、あるいは２０８バイトのデータ全体に対して、前述したようなデータ変換を行うことにより暗号化を施すことができる。このデータ変換は、前述したように、端子２１８を介して入力される鍵情報に応じて施すようにしてもよい。また、データ変換回路２１５については、ＰＩエンコーダ２１４が各行の１７２バイトのデータに対して、それぞれ１０バイトずつのＰＩパリティを付加して１８２バイトのデータを出力することから、この１０バイトのパリティに対して、あるいは１８２バイトのデータ全体に対してデータ変換を行うことにより暗号化を施すことができる。このデータ変換も、前述したように、端子２１９を介して入力される鍵情報に応じて施すようにしてもよい。

【００８４】上記データ変換は、具体的には、前記図１０、図１１、図１２と共に説明したように、インバータを所定位置に配設したり、ExOR回路群により鍵情報に応じて選択的にデータを反転させたり、その他、ＡＮＤ、ＯＲ、NAND、NOR 回路群等を使用してもよい。また、８ビット単位で１ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、８ビットの情報データに対して８ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの１ワードに相当する８ビットの内の各ビットに対してそれぞれＡＮＤ、ＯＲ、ExOR、NAND、NOR 、インバート回路を組み合わせて使用してもよい。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。また、ＡＮＤ、ＯＲ、ExOR、NAND、NOR 、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。また、シフトレジスタを用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。

【００８５】誤り訂正符号化された上記１８２バイト×２０８行のデータは、行についてインターリーブされ、１３行ずつ１６のグループに分けられて、各グループが記録セクタに対応付けられる。１セクタは、１８２バイト×１３行の２３６６バイトとなるが、これらが変調されて、図２９に示すように１行当たり２つの同期コードＳＹが付加される。変調には、前述した第１の実施の形態と同様に８－１６変換が用いられるが、１行は２つのシンクフレームに分けられ、１シンクフレームは、３２チャネルビットの同期コードＳＹと１４５６チャネルビットのデータ部とから成っている。図２９は、変調され同期付加されて得られた１セクタ分の構造を示し、この図２９に示す１セクタ分の３８６８８チャネルビットは、変調前の２４１８バイトに相当する。

【００８６】図２９の変調出力信号には、８種類の同期コードＳＹ０～ＳＹ７が用いられており、これらの同期コードＳＹ０～ＳＹ７は、上記８－１６変換の状態（ステート）に応じて、ステート１及び２のときが図３０の（ａ）、ステート３及び４のときが図３０の（ｂ）の同期パターンとなっている。

【００８７】このような８種類の同期コードＳＹ０～ＳＹ７の選択を、例えば図３１に示すような回路を用いて、３ビットの鍵情報に応じて変更することにより、暗号化が行える。すなわち、上記８種類の同期コードＳＹ０～ＳＹ７を指定する３ビットデータ２２１の各ビットと、上記３ビットの鍵情報２２２の各ビットとを、３つのExOR回路２２３，２２４，２２５によりそれぞれ排他的論理和をとることにより、新たな同期コード指定データ２２６とする。これにより、上記フレーム構造における同期コードの使い方あるいはフレーム構造内での各種同期コードの使用位置が変更され、暗号化がなされることになる。勿論、その３ビットに対して鍵情報に応じてデータを転置したり、置換したり、シフトレジスタにより変換したりできる。また、これは関数変換でもかまわない。

【００８８】次に、上述した本発明の第２の実施の形態の記録側の構成に対して、再生側の基本構成は、前記図１７と同様であり、上記第２の実施の形態に示した各部の変更箇所に対応して変更された逆処理がそれぞれ施される。例えば、上記図２７に示す誤り訂正符号化に対する逆処理は、図３２のような構成の誤り訂正復号化回路により実現できる。

【００８９】すなわち、この図３２において、入力端子２３０には前記図１７の復調回路１１５からの出力信号であり、上記図２７の出力端子２１６からの出力に相当する上記図２８の積符号の１８２バイト×２０８行のデータが供給されている。この入力端子２３０からのデータは、データ逆変換回路２３１に送られて、上記図２７のデータ変換回路２１５の逆処理が行われる。データ逆変換回路２３１からの出力データは、ＰＩ（内符号）デコーダ２３２に送られて、上記図２７のＰＩエンコーダ２１４の逆処理としての復号化処理すなわちＰＩ符号を用いた誤り訂正処理が施され、上記図２８の１７２バイト×２０８行のデータとなる。ＰＩデコーダ２３２からの出力データは、デインターリーブ回路２３３で上記インターリーブ回路２１３での逆処理が施され、データ逆変換回路２３４に送られて上記図２７のデータ変換回路２１２の逆処理が行われた後、ＰＯ（外符号）デコーダ２３５に送られる。ＰＯデコーダ２３５では、上記図２７のＰＯエンコーダ２１１の逆処理としての復号化処理すなわちＰＯ符号を用いた誤り訂正処理が施され、図２８の元の１７２バイト×１９２行のデータが出力端子２３６を介して取り出される。上記図２７のデータ変換回路２１２、２１５でのデータ変換の際に鍵情報を用いる場合には、各端子２１８、２１９にそれぞれ供給した鍵情報を、図３２のデータ逆変換回路２３４、２３１の各端子２３９、２３８にそれぞれ供給して、これらの鍵情報に応じてデータ逆変換を行わせればよい。

【００９０】以上説明した本発明の第２の実施の形態における効果も、前述した第１の実施の形態の場合と同様である。

【００９１】なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、この他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。また、暗号化の鍵情報に応じてデータを置換したり、転置したり、シフトレジスタ

を用いて変換したり、各種関数演算により変換する等、さまざまな暗号化手法が適用できることは勿論であり、それらを組み合わせて使用することも可能である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【００９２】

【発明の効果】本発明に係るデータ記録方法によれば、入力ディジタルデータを所定データ量単位でセクタ化するセクタ化工程と、ヘッダを付加するヘッダ付加工程と、誤り訂正符号化工程と、所定の変調方式で変調する変調工程と、同期パターンを付加する同期付加工程との、いずれか少なくとも１つの工程について、入力に対して暗号化処理を施して出力するようにしているため、どの工程で暗号化処理が施されたかも暗号の鍵となり、暗号の難易度を高くすることができる。これらの暗号化処理が施され得る工程の１つに、同一パターンを除去するためのランダム化処理を施すスクランブル処理工程を含めてもよい。また、既存の構成の一部を変更するだけで、簡単に暗号化が実現できるという利点もある。これらは、データ記録装置、記録媒体、再生方法及び装置の場合にも得られる効果である。

【００９３】また、本発明によれば、誤り訂正符号化処理の際に取り扱われるデータに対して、暗号化の鍵情報に応じた少なくとも一部のデータにデータ変換を施しているため、誤り訂正処理である程度データ復元が可能な状態から、データ復元が行えない状態までの任意のレベルの暗号化が行える。これによって、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、データ提供の用途に応じた、あるいはセキュリティレベルに応じた対応が可能となる。

【００９４】また、誤り訂正処理の中で鍵のビット数の大きな暗号化が可能であり、誤り訂正符号化や復号化ＩＣあるいはＬＳＩのような巨大なブラックボックスの中で暗号化を実現しているため、一般ユーザによる解読を困難化し、データセキュリティを大幅に向上させることができる。

【００９５】さらに、本発明によれば、所定の鍵情報を用いてデータに対して暗号化処理を施すと共に、この暗号化の鍵情報の少なくとも一部を、記録媒体のデータ記録領域とは別の領域に書き込んでおき、再生時にこの鍵情報の少なくとも一部の情報を読み取って、暗号復号化に用いる。暗号復号化の鍵情報が、記録媒体のデータ記録領域内の情報のみで完結しないため、暗号化の難易度が高まる。

【００９６】またさらに、本発明によれば、　データ列の同一パターンを除去するためのランダム化を主目的とするスクランブル処理の際に、生成多項式及び初期値の少なくとも一方を、暗号化の鍵に応じて変化させることにより、既存のスクランブル処理を暗号化に流用して、簡単な構成で暗号化を実現できる。

【００９７】このようなデータの暗号化により、コピー防止や不正使用の防止が簡単な仕組みで実現でき、またセキュリティや課金システムへも容易に適用できる。

【図面の簡単な説明】

【図１】本発明のデータ記録装置の第１の実施の形態の概略構成を示すブロック図である。

【図２】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック図である。

【図３】偶数・奇数バイトのインターリーブを説明するための図である。

【図４】スクランブラの一例を示す図である。

【図５】スクランブラのプリセット値の一例を示す図である。

【図６】生成多項式が可変のスクランブラの一例を示す図である。

【図７】セクタフォーマットの一例を示す図である。

【図８】セクタ内の同期領域での暗号化の一例を説明するための図である。

【図９】セクタ内のヘッダ領域の一例を示す図である。

【図１０】誤り訂正符号化回路の一例の概略構成を示す図である。

【図１１】誤り訂正符号化回路の一例の具体的な構成を示す図である。

【図１２】誤り訂正符号化回路の他の例を示す図である。

【図１３】変調回路での暗号化処理の一例を説明するための図である。

【図１４】変調信号に付加される同期ワードの具体例を示す図である。

【図１５】同期付加回路での暗号化の一例を説明するための図である。

【図１６】データ記録媒体の一例を示す図である。

【図１７】本発明のデータ再生装置の第１の実施の形態の概略構成を示すブロック図である。

【図１８】復調回路での暗号化処理の一例を説明するための図である。

【図２９】誤り訂正復号化回路の一例の概略構成を示す図である。

【図２０】誤り訂正復号化回路の一例の具体的な構成を示す図である。

【図２１】誤り訂正復号化回路の他の例を示す図である。

【図２２】デスクランブル処理回路の一例を示す図である。

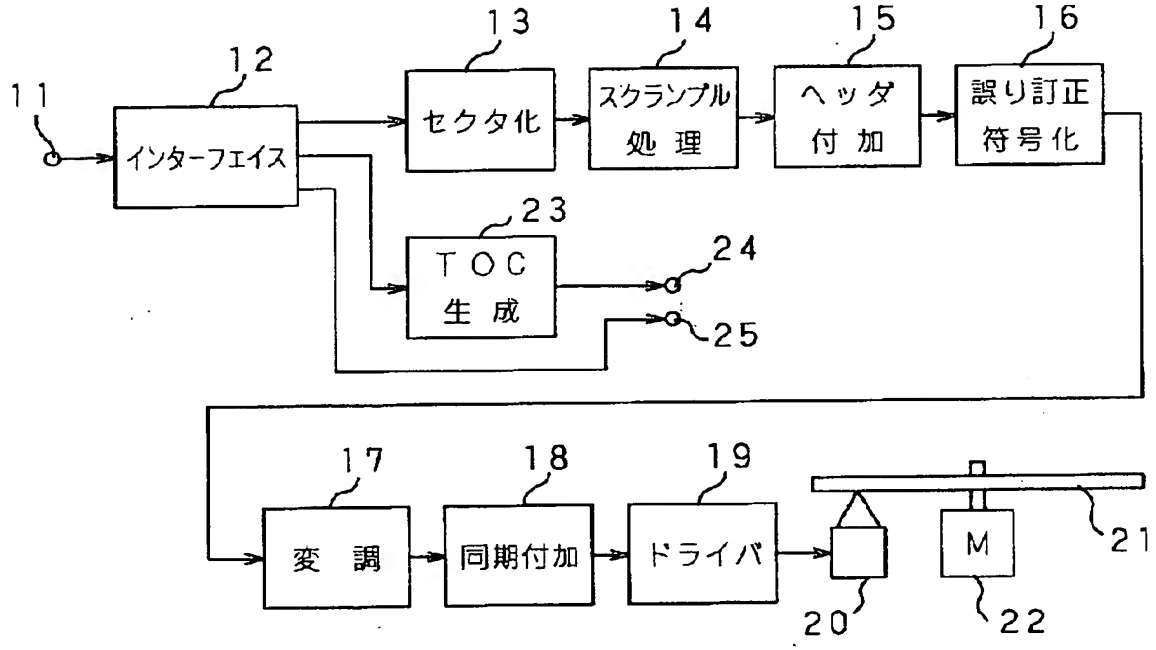
【図２３】スクランブラの他の例を示す図である。

【図２４】図２３のスクランブラのプリセット値の一例を示す図である。

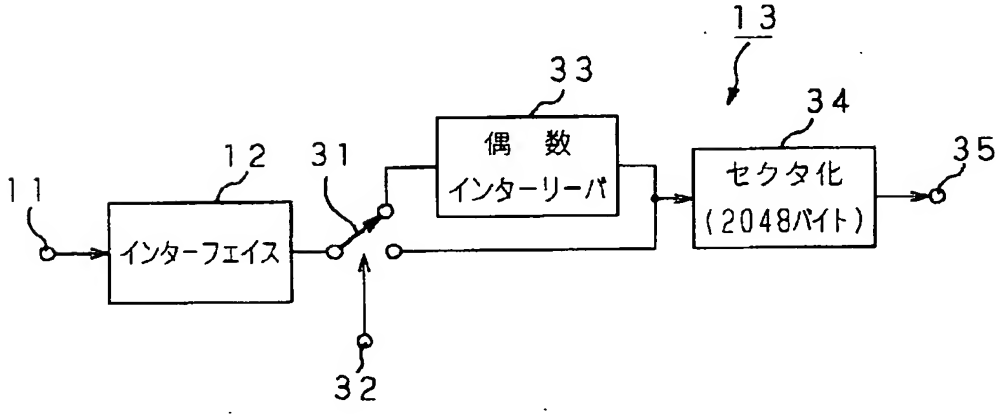
【図２５】セクタフォーマットの他の例を示す図である。

【図２６】図２５のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。
【図２７】誤り訂正符号化回路の他の例を示すブロック図である。
【図２８】誤り訂正符号の具体例としての積符号を示す図である。
【図２９】セクタの信号フォーマットの一例を示す図である。
【図３０】変調信号に付加される同期ワードの他の具体例を示す図である。
【図３１】同期付加回路での暗号化の他の例を説明するための図である。
【図３２】誤り訂正復号化回路の他の例を示すブロック図である。
【符号の説明】
１３　セクタ化回路、　１４　スクランブル処理回路、　１５　ヘッダ付加回路、　１６　誤り訂正符号化回路、　１７　変調回路、　１８　同期付加回路、５７，１４２　再配列回路、　６１，６６，１５１，１５６　ExOR回路群、１１４　同期分離回路、　１１５　復調回路、　１１６　誤り訂正復号化回路、１１７　セクタ分解回路、　１１８　ヘッダ分離回路、　１１９　デスクランブル処理回路

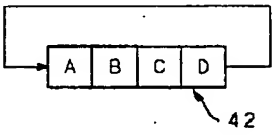
【図１】



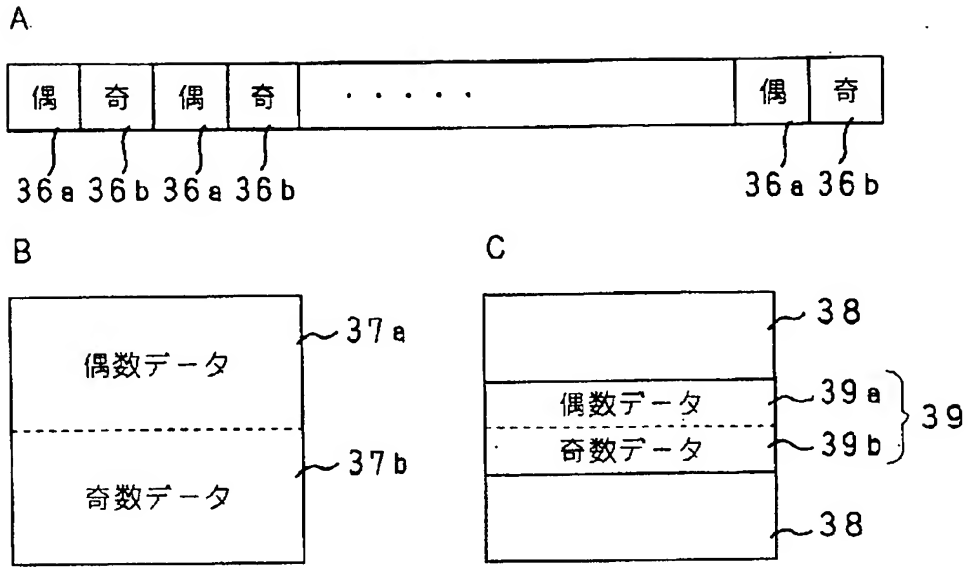
【図２】



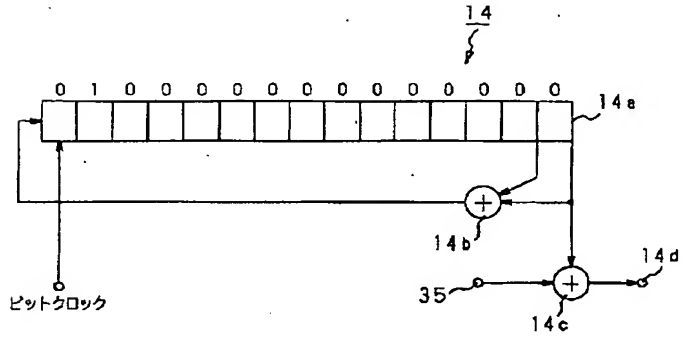
【図８】



【図３】



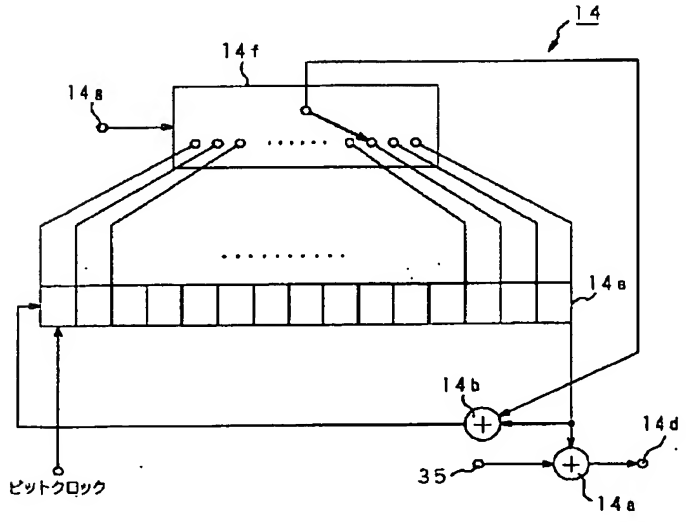
【図４】



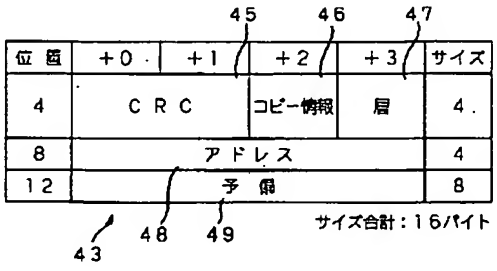
【図５】

選択番号	プリセット値	選択番号	プリセット値
0	$0001	8	$4080
1	$4000	9	$2040
2	$2000	10	$1020
3	$1000	11	$0810
4	$0800	12	$0408
5	$0400	13	$0204
6	$0200	14	$0102
7	$0100	15	$4081

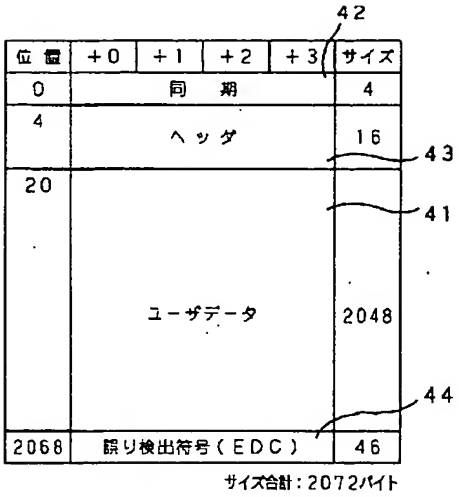
【図６】



【図９】



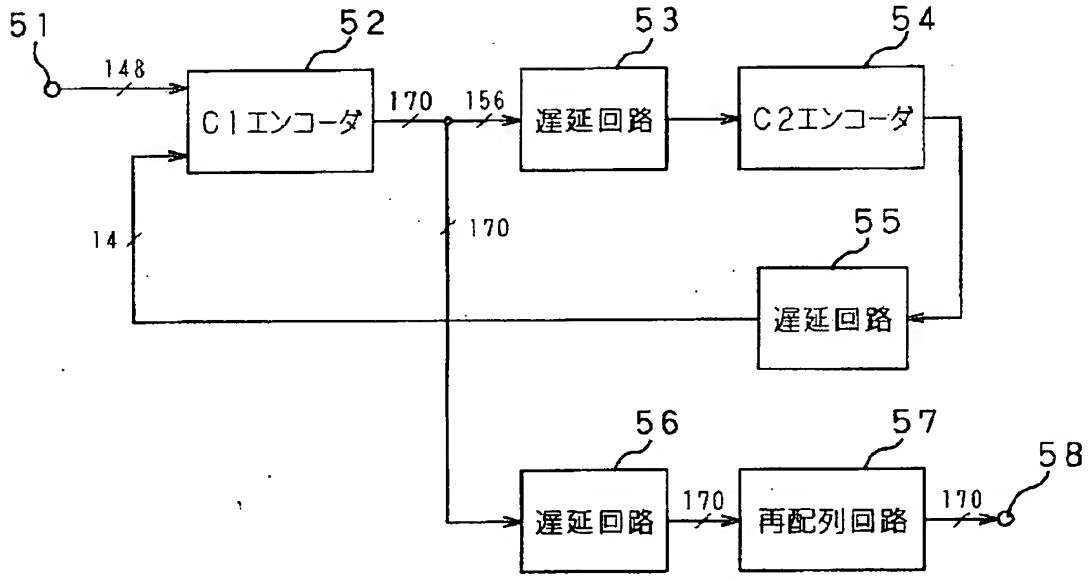
【図７】



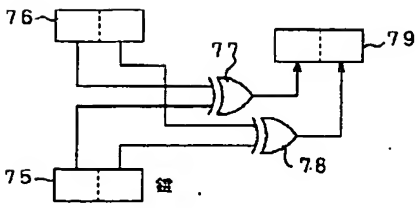
【図１４】

同期ワード	符号ワード	
	msb　同期パターンa　lsb	msb　同期パターンb　lsb
S0	00010010010000000001000000000001	10010010010000000001000000000001
S1	00010000010000000001000000000001	10010000010000000001000000000001
S2	00000100010000000001000000000001	10000100010000000001000000000001
S3	00000100001000000001000000000001	10000100001000000001000000000001

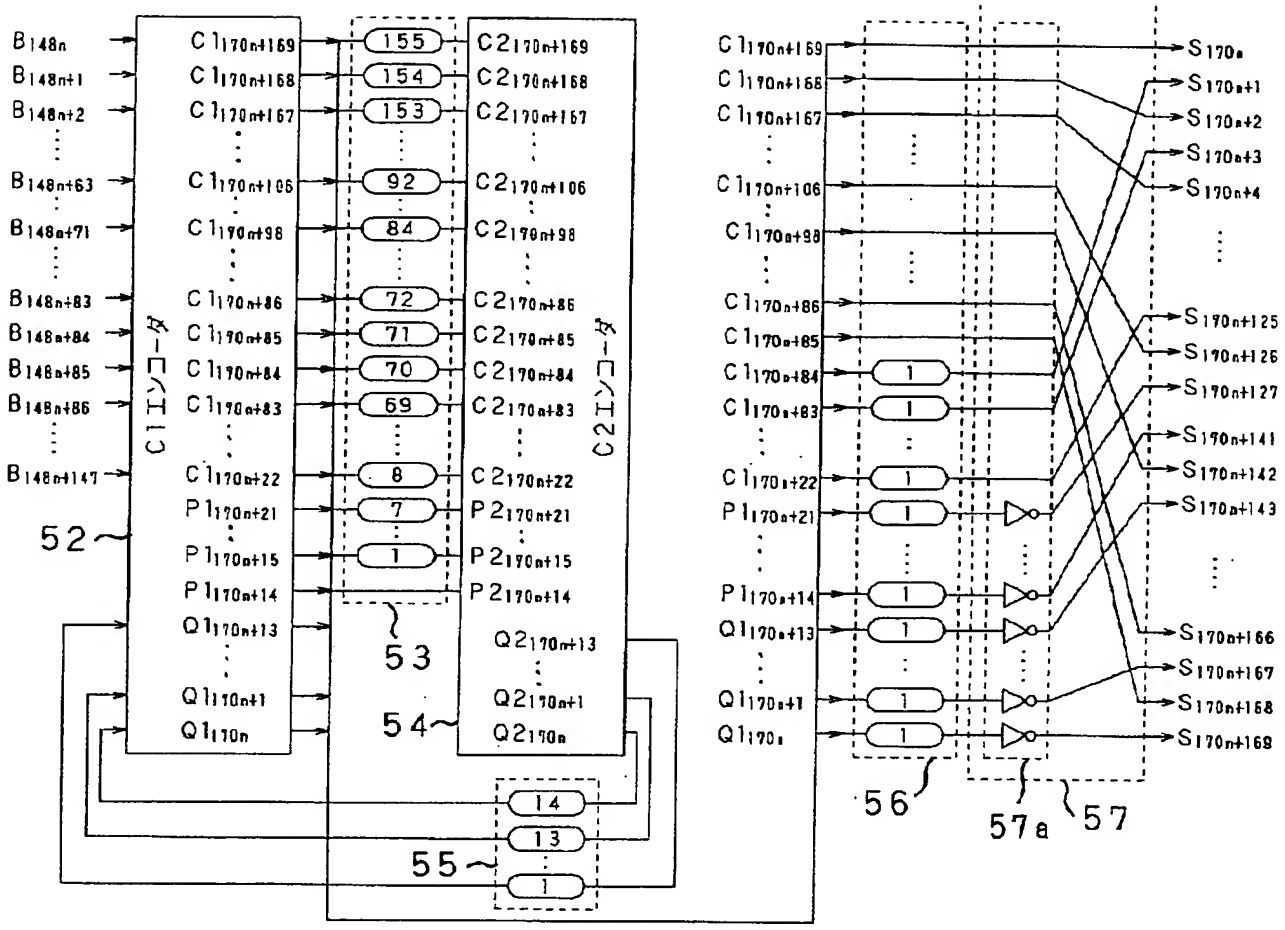
【図１０】



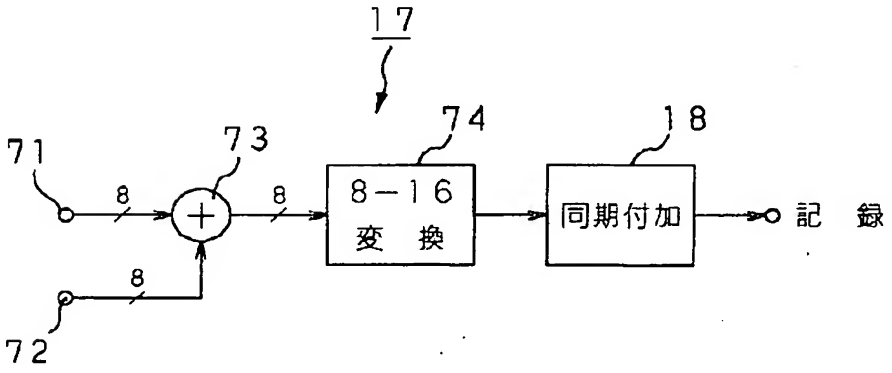
【図１５】



【図１１】



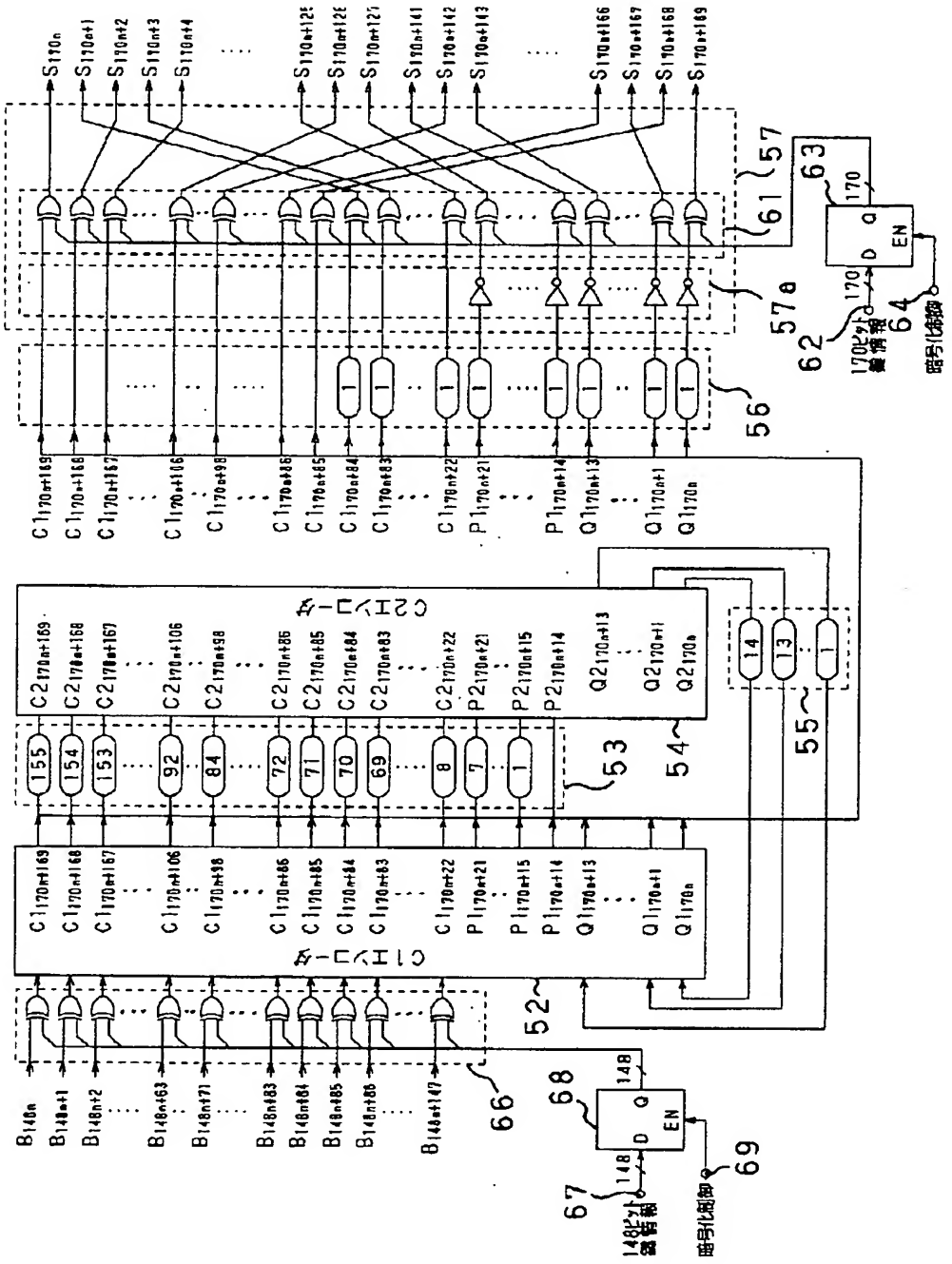
【図１３】



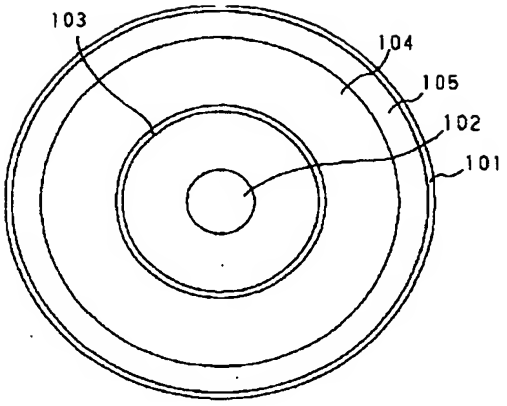
【図２４】

選択番号	プリセット値	選択番号	プリセット値
0	$0001	8	$0010
1	$5500	9	$5000
2	$0002	10	$0020
3	$2A00	11	$2001
4	$0004	12	$0040
5	$5400	13	$4002
6	$0008	14	$0080
7	$2800	15	$0005

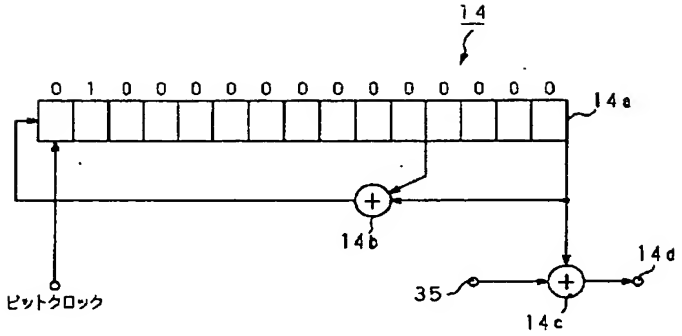
【図１２】


S170n
S170n+1
S170n+2
S170n+3
S170n+4
S170n+125
S170n+126
S170n+127
S170n+141
S170n+142
S170n+143
S170n+166
S170n+167
S170n+168
S170n+169
57
63
170
D
Q
EN
61
57a
62
64
暗号化制御
56
C1170n+169
C1170n+168
C1170n+167
C1170n+106
C1170n+98
C1170n+86
C1170n+85
C1170n+84
C1170n+83
C1170n+22
P1170n+21
P1170n+15
P1170n+14
Q1170n+13
Q1170n+1
Q1170n
C2ドライバ
C2170n+169
C2170n+168
C2170n+167
C2170n+106
C2170n+98
C2170n+86
C2170n+85
C2170n+84
C2170n+83
C2170n+22
P2170n+21
P2170n+15
P2170n+14
Q2170n+13
Q2170n+1
Q2170n
155
154
153
92
84
72
71
70
69
8
7
1
53
54
55
14
13
1
C1ドライバ
52
B148n
B148n+1
B148n+2
B148n+63
B148n+71
B148n+83
B148n+84
B148n+85
B148n+86
B148n+147
66
68
148
67
69

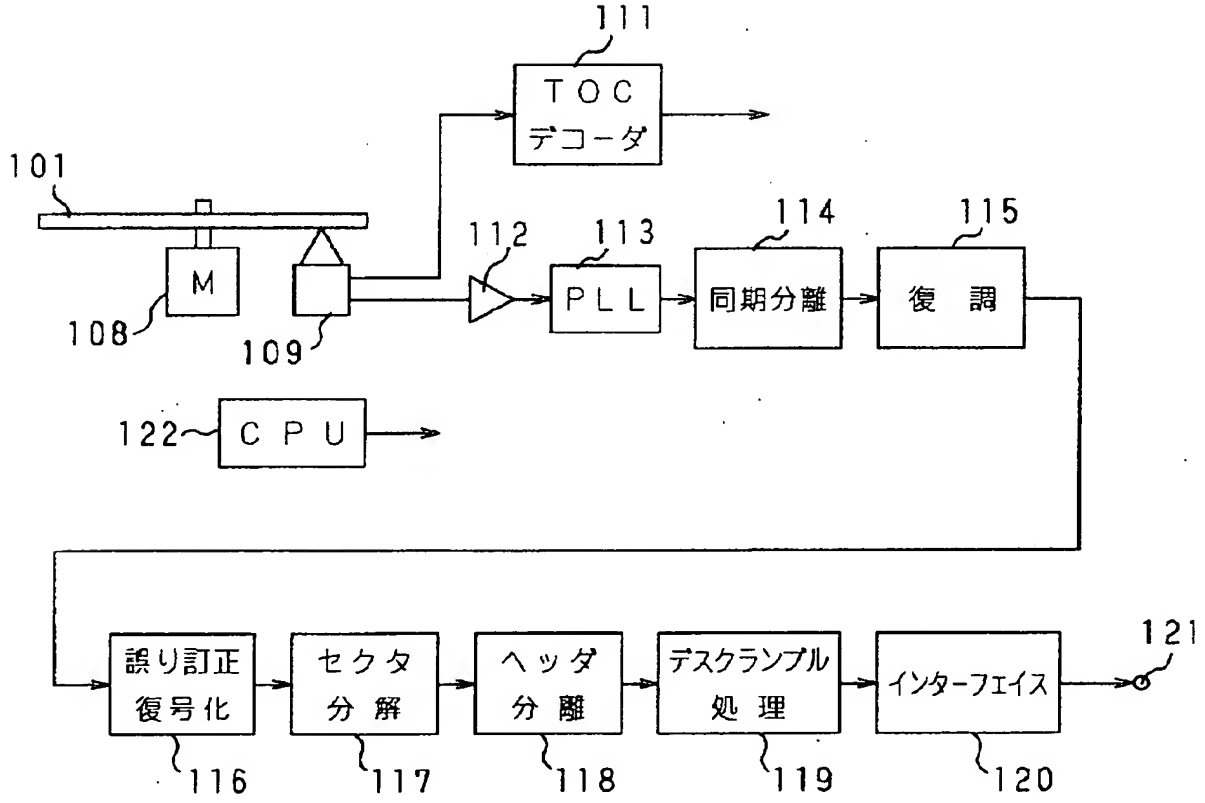
【図１６】


103
104
105
102
101

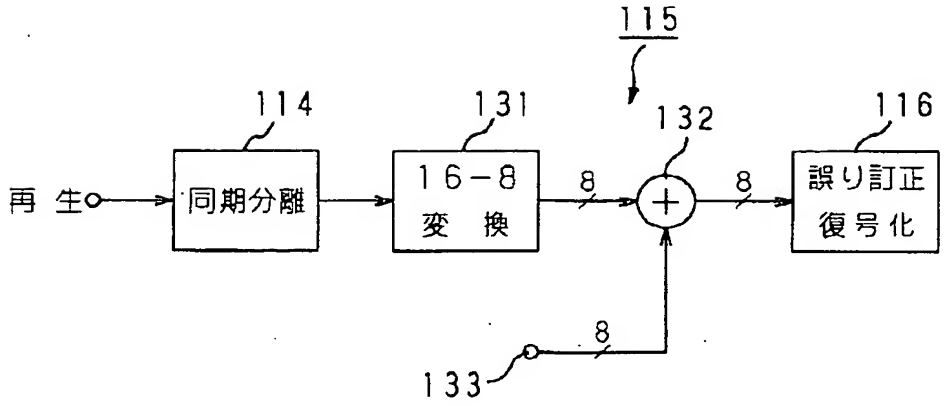
【図２３】


14
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0
14a
14b
14d
35
14c
ビットクロック

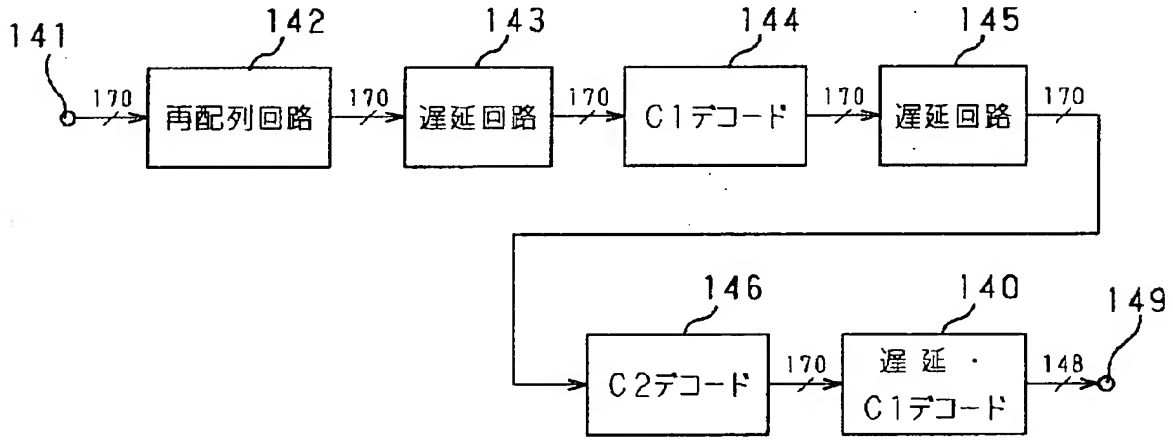
【図１７】


111
TOC
デコーダ
101
M
108
109
112
113
PLL
114
同期分離
115
復　調
122
CPU
誤り訂正
復号化
116
セクタ
分　解
117
ヘッダ
分　離
118
デスクランブル
処　理
119
インターフェイス
120
121

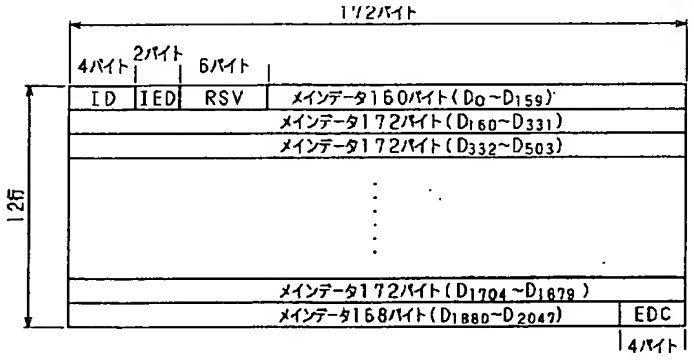
【図１８】



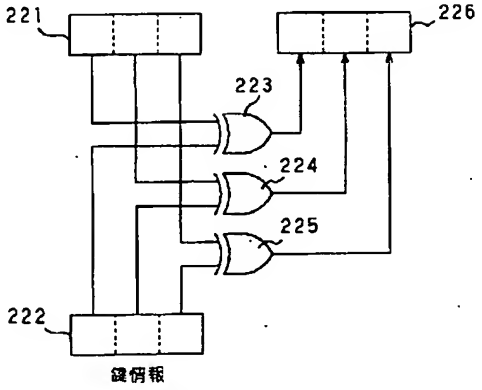
【図１９】



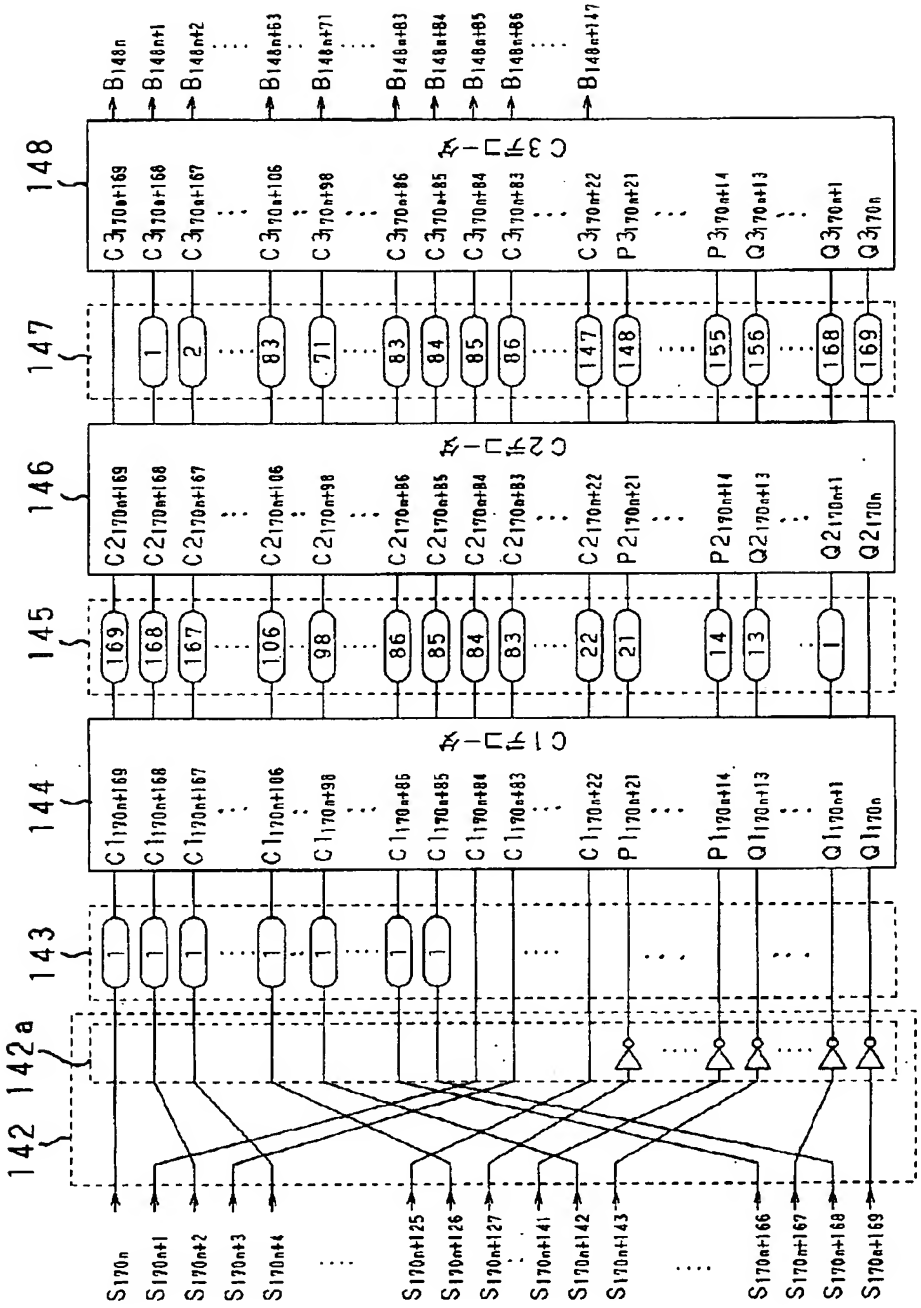
【図２５】



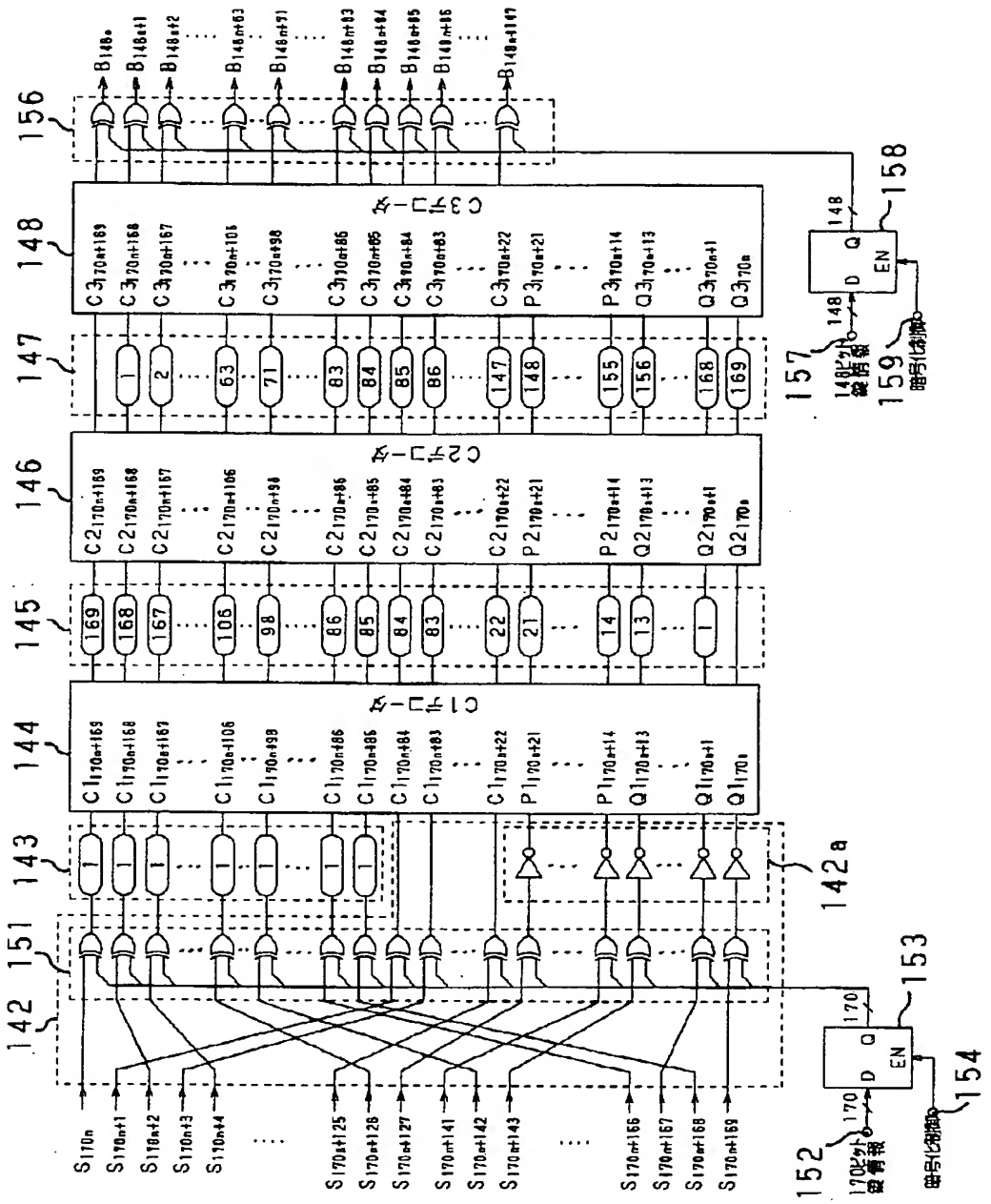
【図３１】



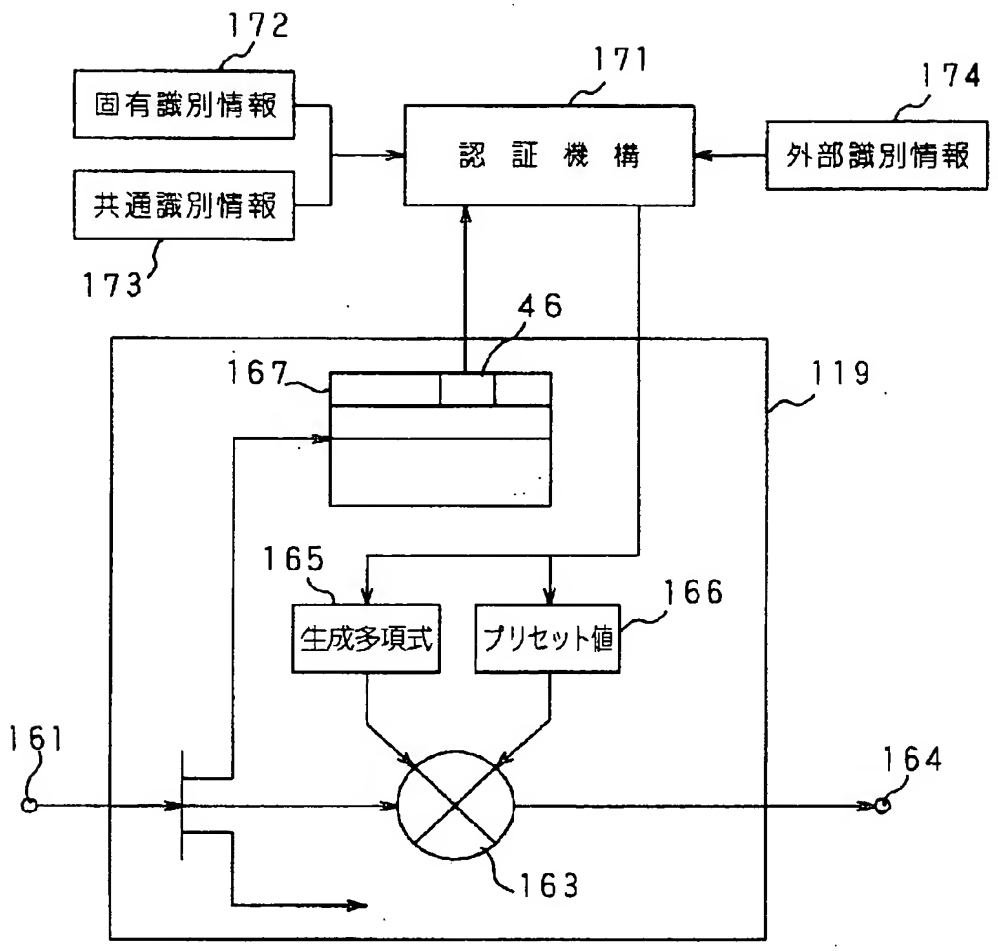
【図２０】



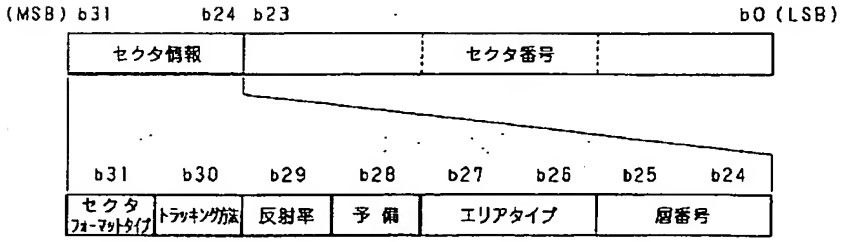
【図２１】


142
142a
143
144
145
146
147
148
151
152
153
154
156
157
158
159
C1ブロック
C2ブロック
C3ブロック
EN
D
Q

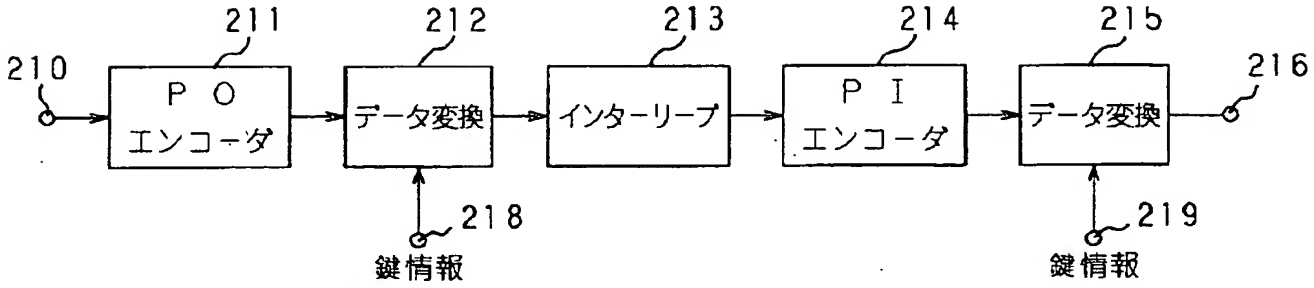
【図２２】


172
固有識別情報
共通識別情報
173
171
認証機構
174
外部識別情報
46
167
119
165
生成多項式
166
プリセット値
161
164
163

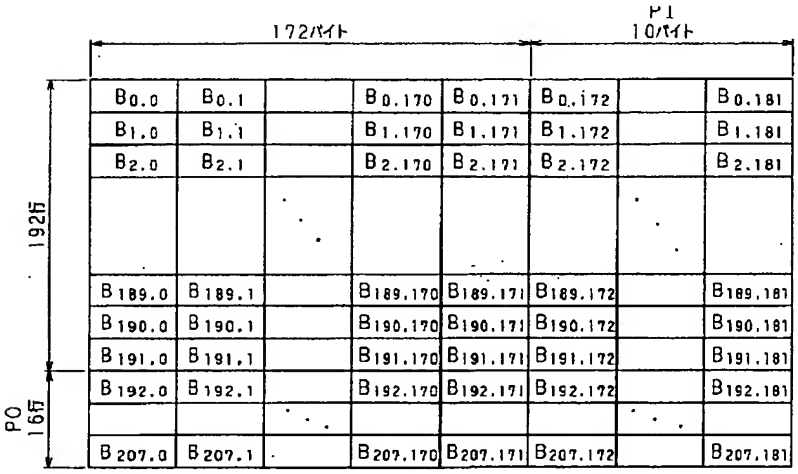
【図２６】


(MSB) b31
b24 b23
b0 (LSB)
セクタ情報
セクタ番号
b31 b30 b29 b28 b27 b26 b25 b24
セクタフォーマットタイプ
トラッキング方法
反射率
予備
エリアタイプ
層番号

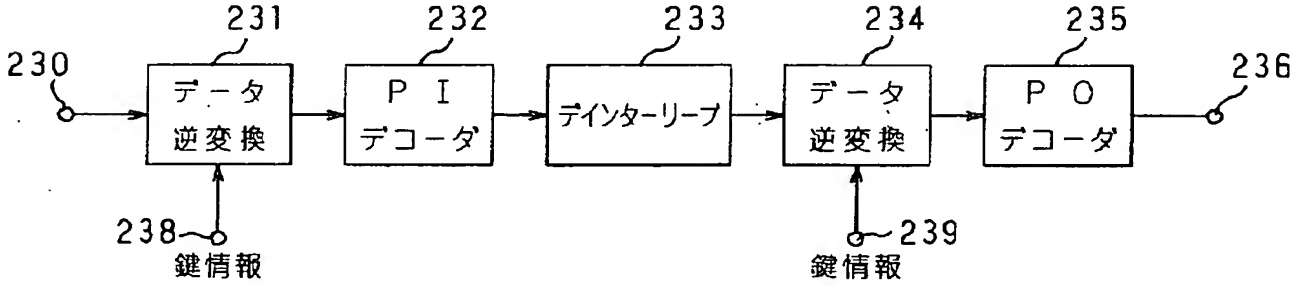
【図２７】


210
211
P O
エンコーダ
212
データ変換
213
インターリーブ
214
P I
エンコーダ
215
データ変換
216
218
鍵情報
219
鍵情報

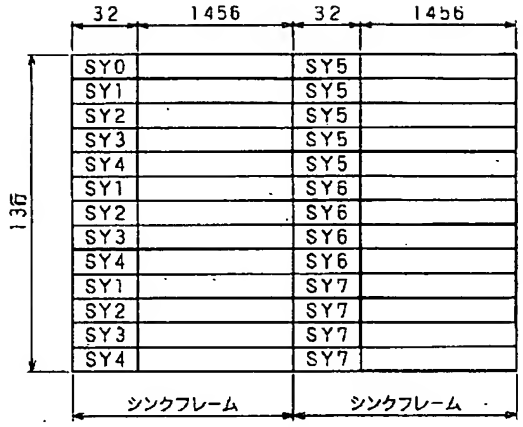
【図２８】


172バイト
PI
10バイト
192行
PO
16行
B0.0 B0.1 B0.170 B0.171 B0.172 B0.181
B1.0 B1.1 B1.170 B1.171 B1.172 B1.181
B2.0 B2.1 B2.170 B2.171 B2.172 B2.181
B189.0 B189.1 B189.170 B189.171 B189.172 B189.181
B190.0 B190.1 B190.170 B190.171 B190.172 B190.181
B191.0 B191.1 B191.170 B191.171 B191.172 B191.181
B192.0 B192.1 B192.170 B192.171 B192.172 B192.181
B207.0 B207.1 B207.170 B207.171 B207.172 B207.181

【図３２】


230
231
データ
逆変換
232
P I
デコーダ
233
デインターリーブ
234
データ
逆変換
235
P O
デコーダ
236
238
鍵情報
239
鍵情報

【図２９】



【図３０】

(a)ステート1及び2

	(MSB)	(LSB)	(MSB)	(LSB)
SY0=	0001001001000100	0000000000010001	0001001000000100	0000000000010001
SY1=	0000010000000100	0000000000010001	0000010001000100	0000000000010001
SY2=	0001000000000100	0000000000010001	0001000001000100	0000000000010001
SY3=	0000100000000100	0000000000010001	0000100001000100	0000000000010001
SY4=	0010000000000100	0000000000010001	0010000001000100	0000000000010001
SY5=	0010001001000100	0000000000010001	0010001000000100	0000000000010001
SY6=	0010010010000100	0000000000010001	0010000010000100	0000000000010001
SY7=	0010010001000100	0000000000010001	0010010000000100	0000000000010001

(b)ステート3及び4

	(MSB)	(LSB)	(MSB)	(LSB)
SY0=	1001001000000100	0000000000010001	1001001001000100	0000000000010001
SY1=	1000010001000100	0000000000010001	1000010000000100	0000000000010001
SY2=	1001000001000100	0000000000010001	1001000000000100	0000000000010001
SY3=	1000001001000100	0000000000010001	1000001000000100	0000000000010001
SY4=	1000100001000100	0000000000010001	1000100000000100	0000000000010001
SY5=	1000100100000100	0000000000010001	1000000100000100	0000000000010001
SY6=	1001000010000100	0000000000010001	1000000001000100	0000000000010001
SY7=	1000100010000100	0000000000010001	1000000010000100	0000000000010001

【手続補正書】
【提出日】平成８年７月１９日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】図面の簡単な説明
【補正方法】変更
【補正内容】
【図面の簡単な説明】
【図１】本発明のデータ記録装置の第１の実施の形態の概略構成を示すブロック図である。
【図２】セクタ化回路における偶数・奇数バイトのインターリーブを実現するための構成例を示すブロック図である。
【図３】偶数・奇数バイトのインターリーブを説明するための図である。
【図４】スクランブラの一例を示す図である。
【図５】スクランブラのプリセット値の一例を示す図で

ある。
【図６】生成多項式が可変のスクランブラの一例を示す図である。
【図７】セクタフォーマットの一例を示す図である。
【図８】セクタ内の同期領域での暗号化の一例を説明するための図である。
【図９】セクタ内のヘッダ領域の一例を示す図である。
【図１０】誤り訂正符号化回路の一例の概略構成を示す図である。
【図１１】誤り訂正符号化回路の一例の具体的な構成を示す図である。
【図１２】誤り訂正符号化回路の他の例を示す図である。
【図１３】変調回路での暗号化処理の一例を説明するための図である。
【図１４】変調信号に付加される同期ワードの具体例を示す図である。
【図１５】同期付加回路での暗号化の一例を説明するための図である。
【図１６】データ記録媒体の一例を示す図である。
【図１７】本発明のデータ再生装置の第１の実施の形態の概略構成を示すブロック図である。
【図１８】復調回路での暗号化処理の一例を説明するための図である。
【図１９】誤り訂正復号化回路の一例の概略構成を示す図である。
【図２０】誤り訂正復号化回路の一例の具体的な構成を示す図である。
【図２１】誤り訂正復号化回路の他の例を示す図である。
【図２２】デスクランブル処理回路の一例を示す図である。
【図２３】スクランブラの他の例を示す図である。
【図２４】図２３のスクランブラのプリセット値の一例を示す図である。
【図２５】セクタフォーマットの他の例を示す図である。
【図２６】図２５のセクタフォーマットにおけるセクタ内のヘッダ領域の一例を示す図である。
【図２７】誤り訂正符号化回路の他の例を示すブロック図である。
【図２８】誤り訂正符号の具体例としての積符号を示す図である。
【図２９】セクタの信号フォーマットの一例を示す図である。
【図３０】変調信号に付加される同期ワードの他の具体例を示す図である。
【図３１】同期付加回路での暗号化の他の例を説明するための図である。
【図３２】誤り訂正復号化回路の他の例を示すブロック図である。
【符号の説明】
１３　セクタ化回路、　１４　スクランブル処理回路、　１５　ヘッダ付加回路、　１６　誤り訂正符号化回路、　１７　変調回路、　１８　同期付加回路、５７，１４２　再配列回路、　６１，６６，１５１，１５６　ExOR回路群、１１４　同期分離回路、　１１５　復調回路、　１１６　誤り訂正復号化回路、１１７　セクタ分解回路、　１１８　ヘッダ分離回路、　１１９　デスクランブル処理回路

フロントページの続き

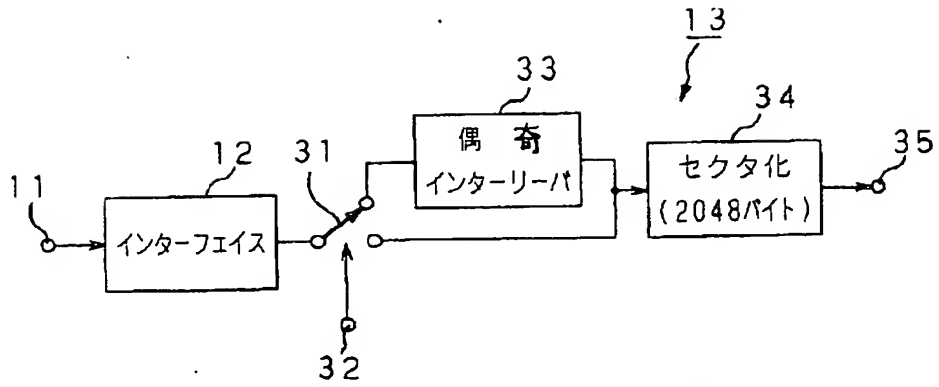
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　応和　英男
東京都品川区北品川６丁目７番35号　ソニー株式会社内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１４年２月２８日（２００２．２．２８）

【公開番号】特開平９－７３４１４
【公開日】平成９年３月１８日（１９９７．３．１８）
【年通号数】公開特許公報９－７３５
【出願番号】特願平８－９８９４９
【国際特許分類第７版】
G06F 12/14 320
G09C 1/00 660
G11B 20/10
20/12 102
20/18 570
【ＦＩ】
G06F 12/14 320 B
G09C 1/00 660 D
G11B 20/10 H
20/12 102
20/18 570 N

【手続補正書】
【提出日】平成１３年７月１９日（２００１．７．１９）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正内容】
【００２６】先ず、セクタ化回路１３においては、例えば図２に示すような偶数・奇数バイトのインターリーブ処理を行わせることが挙げられる。すなわち、図２において、上記図１のインターフェース回路１２からの出力を、２出力の切換スイッチ３１に送り、この切換スイッチ３１の一方の出力を偶奇インターリーバ３３を介してセクタ化器３４に送り、切換スイッチ３１の他方の出力をそのままセクタ化器３４に送っている。セクタ化器３４では、例えば入力データの２０４８バイト単位でまとめて１セクタとしている。このセクタ化回路１３の切換スイッチ３１の切換動作を、鍵となる１ビットの制御信号で制御するわけである。偶奇インターリーバ３３は、図３のＡに示すような偶数バイト３６ａと奇数バイト３６ｂとが交互に配置された入力データの１セクタ分を、図３のＢに示すように、偶数データ部３７ａと奇数データ部３７ｂとに分配して出力する。さらに、図３のＣに示すように、１セクタ内の所定の領域３９を鍵情報により特定し、この領域３９内のデータについてのみ偶数データ部３９ａと奇数データ部３９ｂとに分配するようにしてもよい。この場合には、領域３９の特定の仕方を複数通り選択できるように設定することもでき、鍵情報の選択肢をさらに増加させて暗号化のレベルをより高めることもできる。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正内容】
【図２】



【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図６
【補正方法】変更
【補正内容】
【図６】